U.S. DoD Remote Access Protection Profile for SBU-High Environments

Version 0.9

May 27, 2000

Prepared By:
Booz·Allen & Hamilton Inc.
900 Elkridge Landing Road
Linthicum, MD 21090

Foreword

Protection Profile Title: U.S. DoD Remote Access Protection Profile for SBU-High Environments.

Criteria Version:

This protection profile (PP) was developed using Version 2.1 of the Common Criteria (CC) [1].

Constraints:

Targets of Evaluation (TOEs) developed to satisfy this Protection Profile shall conform to CC Part 2 and CC Part 3.

Authors:

This Protection Profile was prepared by:

Brian Green

John Gurzick

Steve Hutchens

Janine Meehan

Angela Streeter

Mike Alexander

Acknowledgements:

Table Of Contents

List of Tables

List of Figures

Conventions and Terminology

Conventions

COMMON CRITERIA PRESENTATION CONVENTIONS

The notation, formatting, and conventions used in this protection profile (PP) are based on or consistent with version 2.1 of the Common Criteria (CC). Font style and clarifying information conventions were developed to aid the reader. Additionally, British English is used throughout the protection profile.

A font style convention was developed so that protection profiles will be consistent in the presentation of functional component operations. The family behaviour name is followed by the family short name in parentheses, and the short family name is superscripted following the requirement statement, e.g.:

Audit Review (FAU_SAR.1)

The TSF shall provide [an authorised administrator] with the capability to read [all trail data] from the audit records. $^{\text{FAU\_SAR.1.1}}$

The CC permits four functional component operations—assignment, iteration, refinement, and selection—to be performed on functional requirements. These operations are defined in Common Criteria, Part 2, paragraph 2.1.4 as

- assignment: allows the specification of an identified parameter;
- iteration: allows a component to be used more than once with varying operations;
- refinement: allows the addition of details; and
- selection: allows the specification of one or more elements from a list.

With the exception of iteration, these operations are expressed by using bolded, italicised, and underlined text. The author used brackets ("[]") to set off all assignments or selections that require future action by the developer. The text "assignment:" or "selection:" is indicated within the brackets. Iterations are set off with parentheses. The iteration "(#)" follows the short family name and "(iteration #)" follows the family behaviour.

Table 1-1 Functional Requirements Operation Conventions

Convention	Purpose	Operation
Bold	The purpose of bolded text is used to alert the reader that additional text has been added to the CC. Example: The TSF shall export **(in ASCII format)** the **labelled** user data with the user data's associated security attributes.	Assignment Refinement
Italics	The purpose of italicised text is to inform the reader of an appended assignment or selection operation to be completed by the developer. Example: The TSF shall provide the following [assignment: *list of additional SFP capabilities*].	Assignment Selection
Underline	The purpose of underlined text is to inform the reader that a choice was made from a list provided by the CC selection operation statement. Example: The TSF shall be able to prevent modifications to the audit records.	Selection
Bold & Italics	The purpose of bolded and italicised text is to inform the reader that the author has added new text to the requirement and that an additional vendor action needs to be taken. Example: **Subject sensitivity label; Object sensitivity label; [assignment: *list of additional attributes that audit selectivity is based upon*].**	Assignment Refinement

Convention	Purpose	Operation
Parentheses	The purpose of using parentheses and an iteration number is to inform the reader that the author has selected a new field of assignments or selections with the same requirement and that the requirement will be used multiple times. Example: Basic data exchange confidentially (Iteration 1) FDP_UCT.1(1) The TSF shall enforce the **[policies P.ADMIN ACCESS and P.USER ACCESS]** to be able to transmit objects in a manner protected from unauthorised disclosure. FDP_UCT.1.1 Basic data exchange confidentially (Iteration 2) FDP_UCT.1(2) The TSF shall enforce the **[policies P.ADMIN ACCESS and P.USER ACCESS]** to be able to receive objects in a manner protected from unauthorised disclosure. FDP_UCT.1.1	Iteration

Convention	Purpose	Operation
Endnotes	The purpose of endnotes is to alert the reader that the author has deleted Common Criteria text. An endnote number is inserted at the end of the requirement, and the endnote is recorded on the last page of the section. The endnote statement first states that a deletion was performed and then provides the rationale. Following is the family behaviour or requirement in its original and modified form. A strikethrough is used to identify deleted text and bold for added text. A text deletion rationale is provided. Examples: Text as shown: **Guarantees of audit data availability** (FAU_SGT.1) [1] Endnote statement: A deletion of CC text was performed. Rationale: The component name was changed to …. ~~Protected audit trail storage~~ **Guarantees of audit data availability** (FAU_SGT.1) Text as shown: The TSF shall **be able to** prevent auditable events, except those taken by the authorised administrator, and **[assignment: *other actions to be taken in case of audit storage*]** if the audit trail is full. (FAU_STG.4.1) [2] Endnote statement: A deletion of CC text was performed. Rationale: The words "with special rights" were deleted because …. The TSF shall **be able to** prevent auditable events, except those taken by the authorised administrator ~~with special rights~~, and **[assignment: *other actions to be taken in case of audit storage*]** if the audit trail is full. (FAU_STG.4.1)	Refinement

Convention	Purpose	Operation
(EXP)	The purpose of using (EXP) after the family behaviour name is to alert the reader to and explicitly identify a newly created requirement. Example. **Object security attributes (EXP)** (FDP_OSA.1) **The TSF shall associate the following security attributes with named objects:** **a) Access control attributes, consisting of the following [assignment: *list of object attributes used to enforce the Discretionary Access Control Policy*.]** **b) Sensitivity label consisting of a hierarchical level and a set of non-hierarchical categories** **c) [assignment: *other object security attributes*]. (EXP)** (FDP_OSA.1.1)	Refinement

As a means to provide the reader with additional requirement understanding or to clarify the author's intent, requirements overview and application notes are used.

The requirements overview are used to provide a discussion of the relationship between functional requirements so that the protection profile reader can understand why a component or group of components were chosen and what effect they are expected to have as a group of related functions. The requirements overview precedes either a component or a set of components.

To provide support information that is considered relevant or useful for the construction, evaluation, or use of the Target of Evaluation (TOE), e.g., to clarify the intent of a requirement, to identify implementation choices, or to define "pass-fail" criteria for a requirement, application notes are used. Application notes follow the relevant requirement component.

NAMING CONVENTIONS

Explicit Requirements: The Common Criteria paradigm allows protection profile and security target authors to create their own requirements, termed explicit requirements, should the Common Criteria not offer suitable requirements to meet their needs. Explicit requirements must be identified and are required to use the Common Criteria class/family/component model in articulating these requirements. The naming convention for explicit requirements is the same as that used in the Common Criteria. There is a long name that is easily associated with the context of the requirement, and there is a short name, i.e., wxx_yy.c.d, where w = F for function; A for assurance; xx = the class name; yyy = the component name; c = component; and d = element. To ensure these requirements are explicitly identified, the parenthetical phrase (EXP) is appended to the newly created short name. The newly created explicit requirements are integrated with the CC requirements in alphabetical order by short name. The rationale for creating a requirement is provided in Section 6.6 Explicit Requirements Rationale.

Assumptions: TOE security environment assumptions are given names beginning with "A." and are presented in alphabetical order, e.g., A.ENCRYPT, A.NOPUBLIC.

Threats: TOE security environment threats are given names beginning with "T."and are presented in alphabetical order, e.g., T.ASPOOF, T.IMPORT .

Policies: TOE security environment policies are given names beginning with "P." and are presented in alphabetical order, e.g., P.NEED_TO_KNOW, P.TRAINING.

Objectives: Security objectives for the TOE and the TOE environment are given names beginning with "O." and "OE." respectively and are presented in alphabetical order, e.g., O.AUDITING, O.RESIDUAL_INFORMATION, OE.BACKUP.

Terminology

The following list of commonly used terms is presented here to aid the reader:

Administrator	Human user to whom authorisation has been granted to perform administrative and security operations that affect the enforcement of the site's TOE security policy (TSP).
Agent	Any authorised or unauthorised user.
Authorised User	Any person (or process acting on behalf of a person) who is outside the boundary of the Target of Evaluation (TOE), who is authorized to interact with the TOE. Authorized Users (AUs) are trusted. However occasionally they may prove themselves to be untrustworthy, in which case they are referred to as an Unauthorized Agent (UA).
Component	The smallest selectable set of elements that may be included in a PP, an ST, or a package.
Dependency	A relationship between requirements such that the requirement that is depended upon must normally be satisfied for the other requirements to be able to meet their objectives.
Element	Members of a component; cannot be selected individually.
Evaluation Assurance Level (EAL)	A package consisting of assurance components from CC, Part 3 that represents a point on the CC predefined assurance scale.
Object	An entity within the TOE Security Functions Scope of Control (TSC) that contains or receives information and upon which subjects perform operations.

Package

A reusable set of either functional or assurance components (e.g., an EAL), combined together to satisfy a set of identified security objectives.

Protection Profile (PP)

An implementation-independent set of security requirements for a category of TOEs that meet specific consumer needs.

Security Target (ST)

A set of security requirements and specifications to be used as the basis for evaluation of an identified TOE.

Sensitive Information

Information that requires protection, because the information’s content is either sensitive or distribution is restricted. Loss or modification of the sensitive information may cause damage to the security, safety, financial posture, and/or infrastructure of the organisation. Organisations, both inside and outside of government seek to protect information of this type. For example, in a DoD environment sensitive information might be information related to the provisioning of military supplies such as bullets or fuel to deployed forces. Sensitive information as used herein, is unclassified, more important than routine administrative information, and less important than mission critical information.

Subject

An entity within the TSC that causes operations to be performed.

Target of Evaluation (TOE)

An IT product or system and its associated administrator and user guidance documentation that is the subject of an evaluation.

TOE Security Functions (TSF)

A set consisting of all hardware, software, and firmware of the TOE that must be relied upon for the correct enforcement of the TSP.

TOE Security Policy (TSP)

A set of rules that regulate how assets are managed, protected, and distributed within a TOE.

TSF Scope of Control (TSC)

The set of interactions that can occur with or within a TOE and are subject to the rules of the TOE security policy.

Unauthorised User

Any person that is not authorised under the TOE security policy to access the TOE.

Document Organisation

Section 1 provides the introductory material for the protection profile.

Section 2 provides general purpose and TOE description.

Section 3 provides a discussion of the expected environment for the TOE. This section also defines the set of threats that are to be addressed by either the technical countermeasures implemented in the TOE hardware or software or through the environmental controls.

Section 4 defines the security objectives for both the TOE and the TOE environment.

Section 5 contains the functional and assurance requirements derived from the Common Criteria, Part 2 and 3, respectively, that must be satisfied by the TOE.

Section 6 provides a rationale to explicitly demonstrate that the information technology security objectives satisfy the policies and threats. Arguments are provided for the coverage of each policy and threat. The section then explains how the set of requirements are complete relative to the objectives, and that each security objective is addressed by one or more component requirements. Arguments are provided for the coverage of each objective. Next, Section 6 provides a set of arguments that address dependency analysis, strength of function issues, and the internal consistency and mutual supportiveness of the protection profile requirements.

An acronym list is provided to define frequently used acronyms.

A reference section is provided to identify background material.

1—Introduction

This protection profile was sponsored by the National Security Agency, Network Security Group, to develop a SBU *system-level* protection profile. Remote Access, one of the sections of the Information Assurance Technical Framework (IATF), was selected as the system for the PP because it is believed to be a solution that will be used extensively throughout the DoD community. Thus, this protection profile has been written to address current DoD RASP acquisition of existing "best of breed" technology.

This PP will be of use to several audiences: Information System Security Engineers (ISSEs), product vendors, and system integrators. The primary audience are ISSEs supporting the DoD community in designing secure information systems. The PP defines a minimal set of security requirements upon which a specific implementation of remote access can be built and against which the implementation can be tested. Secondarily, vendors may find this PP to be of value when they write product Security Targets (STs). Finally, system integrators may find this PP useful for identifying areas that need to be addressed to provide a secure system solution, but have not been explicitly dealt with by the products to be used.

Typically, system implementations are composed from a collection of components. A system integrator can then create a system-level Security Target from the STs for the individual components and show, based on compliance with the component STs and further testing, that the composition of components satisfy the system-level ST. Alternatively, component Protection Profiles can be written and the composition shown to satisfy this PP.

The remote access protection profile team drew upon existing documentation that supports remote access solution design, the Information Assurance Technical Framework Release 2.0.1 Section 6.2 (Remote Access), and the existing PPs for Secret-High and High Assurance Environments.

Remote access technology may be used on its own or in conjunction with other security mechanisms to provide a layered security architecture addressing many levels of required security assurance or robustness. Remote access technology typically supports authentication, confidentiality and integrity services.

1.1 Identification

Title: U.S. DoD Remote Access Protection Profile for SBU Environments

Authors: Mike Alexander, Brian Green, John Gurzick, Steve Hutchens, Janine Meehan, Angela Streeter

Vetting Status: Initial Vetting (NSA internal)

CC Version: 2.1 (ISO 15408)

General Status (e.g., active, superseded, retired): Active

Registration: <to be filled in by registry>

Keywords: Remote access, network security, remote unit, communications server

1.2 Protection Profile Overview

This protection profile specifies the U.S. DoD minimum security need for Remote Access connection to a sensitive but unclassified (SBU) system-high enclave via a telephone network (TN) that is outside the sphere of ownership and management of the enterprise making the remote connection. Both the Public Switched Telephone Network (PSTN) and the Defense Switched Network (DSN) can be used by remote access systems that meet this protection profile. Remote access systems addressed by this protection profile are intended to provide a Basic level of assurance to protect Mission Support information. User's should reference DoD Policy Memorandum 6-8510 DoD Information Assurance (hereafter: "GIG Policy"), or CJSCI 6510.01 for more information on requirements for different information and assurance categories.

Remote access solutions described by this PP offer only a single layer of defence and are therefore not appropriate for Mission Critical or High Robustness unless combined with other mechanisms. This PP is written to address the problem of transferring "Mission Support" information between users and enclaves. Based on the characterisation of information as "Mission Support," the GIG policy Implementation Guidance clearly defines minimum assurance levels required for the various security services inherent in a potential solution. Mission Support is defined as "systems handling information that is important to the support of deployed and contingency forces. The information must be absolutely accurate, but can sustain minimal delay without seriously affecting operational readiness or mission effectiveness"(may be classified information, but is more likely to be sensitive, or unclassified information).

The security policy for a specific Remote Access system may dictate extra security requirements with a higher level of assurance. The requirements in this PP also contain several parameters that may be specified to fit the needs of a particular Remote Access system. Since this PP defines requirements for a system, the Target of Evaluation (TOE) may be composed from several inter-connected Security Targets. The PP defines the threats that are to be addressed by a Remote Access system, defines implementation- independent security objectives of the system and its environment, defines the functional and assurance requirements, and provides the rationale for the security objectives.

1.3 Related Protection Profiles

U.S. DoD Remote Access Protection Profile for SECRET-High Environments, Version .8L, October 9, 1998.

> The SBU Remote Access protection profile used the SECRET-High Remote Access protection profile as an initial starting point. The SECRET-High profile is related to this profile in that the environment and basic function of the remote access system is very similar. The SECRET environment adds additional threats and data protection considerations that are not required in the SBU environment.

Remote Access Communications Server Protection Profile for Secret-High Environments, Version 1.0, January 25, 1999.

> The communications server (CS) is a component of a dial-in remote access system. The CS protection profile for SECRET environments is a component of the above Remote

Access System profile for SECRET environments. Again, the SECRET environment adds additional threats and data protection considerations that are not required in the SBU environment.

U.S. DoD Remote Access Protection Profile for High Assurance Environments, Version .99, May 1, 2000.

This protection profile is related to the SBU system profile in the same manner as the SECRET-High Profile described above. High Assurance environments add additional threats and data protection considerations not required at the SBU level.

Virtual Private Network (VPN) Protection Profile for Protecting Sensitive Information, Version 7.5, 16 December, 1999.

A VPN can be used to perform remote access into an enclave across a commercial data network (e.g., the Internet). Therefore, many of the requirements in the VPN PP are similar to those used in this SBU Remote Access PP.

2—TOE Description

A remote access system enables travelling or telecommuting users to securely access their local area networks (LANs), enclaves, or enterprise-computing environments via telephone networks. The communication network is untrusted and may be shared with hostile users. The remote user's computing assets are physically vulnerable, especially when outside the United States, and must be protected. This equipment should be unclassified when it is not in use. An additional requirement is that the user should know when security features are enabled, and more importantly, when they are not!

This Protection Profile supports the case where the accessed enclave is SBU system high, the users have access to the information, and the Telephone Network (TN) connects the user with the enclave. Some requirements, such as those for assurance or cryptographic algorithms, may not be appropriate for information at other levels or for some other form of network.

For the convenience of specifying those requirements that need only apply to a portion of the TOE, there are two distinct TOE partitions that have been identified: a Remote Unit (RU) partition and a Communications Server (CS) partition. A RU contains those parts of the system that a user takes to a remote location, while the CS is the part of the system that remains within the security perimeter of the enclave and connects the enclave with the TN. There may be many Remote Unit partitions in the system, while there is only one Communications Server partition.[1]

Figure 2-1 illustrates the decomposition. The security objectives and specific security functional requirements for this profile will each be identified as either applying to the entire system, the RU partitions, or the CS partition and they will be respectively marked with a subscript of SYS, RU, or CS.[2] This method of partitioning requirements will aid in determining specific objectives and requirements for the component level protection profiles and security targets that make up the composite Remote Access System.

The Enclave Network shown in Figure 2-1 represents the user's local area networks (LANs), enclaves, or enterprise-computing environment. The communications server is tied directly to the enclave network, and is the primary means of access to the enclave for remote users. The communications server funnels information to and from remote users across the telephone network. In the SBU case, the remote users have access to the enclave network as if they were located at a node within the enclave (i.e., at their office). Access is permitted up to the SBU level. The Secure Enclave includes the facility in which the enclave network is located, as well as any physical and personnel protection mechanisms in place.

[1] The use of multiple communications server devices to implement the Communications Server partition is not precluded by this restriction. However, the use of a single Remote Unit to communicate with two distinct Communications Server partitions in separate enclaves is not considered (nor is it precluded) by this profile.

[2] The TN is not treated as a separate partition. The security requirements placed on the TN are expressed as system-level requirements on the communications between TOE partitions and as requirements on the CS and RU partitions. Further details on the rationale for this decision are described in Section 6.6.1 on page 58.

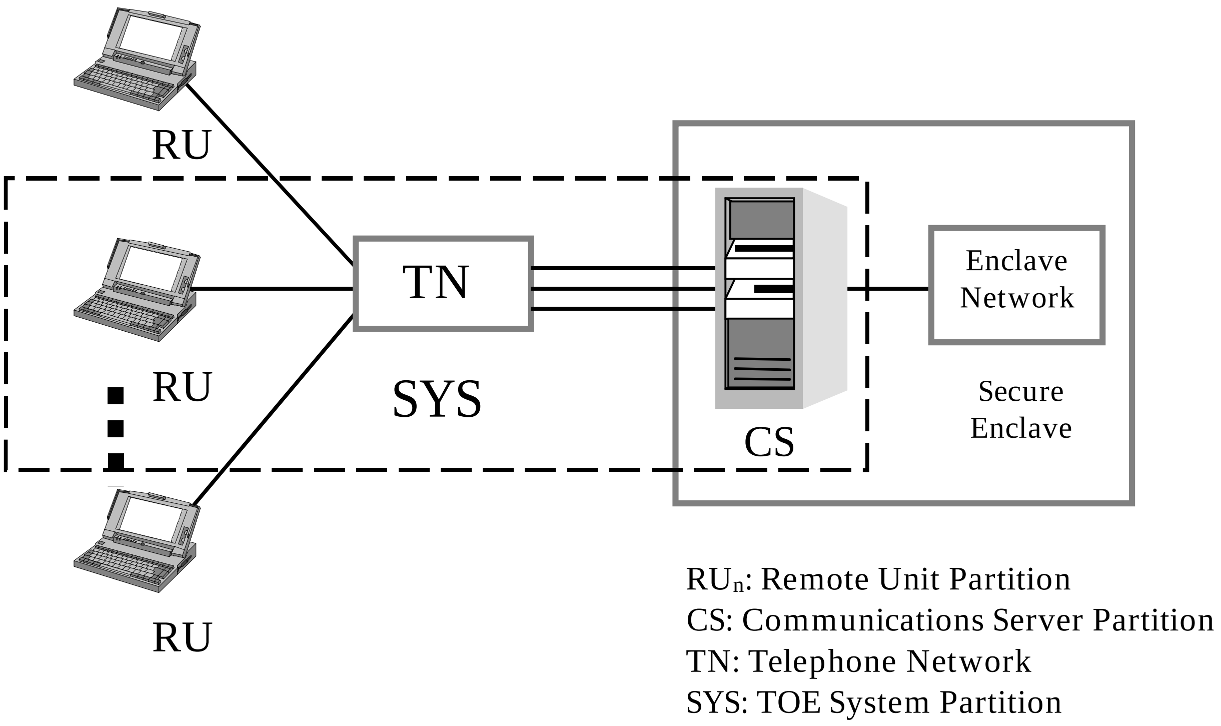
RU
TN
SYS
RU
RU
CS
Enclave Network
Secure Enclave
RU$_n$: Remote Unit Partition
CS: Communications Server Partition
TN: Telephone Network
SYS: TOE System Partition

Figure 2-1 Decomposition of the TOE

The following interfaces exist to the system:

- the user interfaces to the RU (e.g. the keyboard, mouse, display)
- token interfaces: media encryptors provide confidentiality and integrity to the contents of the RU's drive; secure modem authenticates and encrypts the TN connection between the RU and enclave),
- the interface between the RU, the TN and the CS: CS provides network protocol encapsulation after secure connection has been established between two modems (this interface can also be described as a RU-CS interface, once a secure connection has been established),
- the interface of the CS to the backbone network of the enclave: access is granted following proper I&A and application of security features; access is granted to authorised user applications (e.g. email, stored files),
- and (possibly) a direct administrative console interface to the CS.

Any hardware or software required to encrypt/decrypt communications across the TN is considered to be part of the RU or the CS, based on its physical location.

3—TOE Security Environment

The system has a natural decomposition into three distinctly different sub-environments that are part of the system environment: the RU environment local to travelling users and telecommuters, the TN environment, and the environment local to the enclave. The effectiveness of the security functional requirements at mitigating the risks from specific threats and the reliance upon non-IT security objectives has a similar decomposition associated with those three sub-environments. As a result, some of the functional security requirements of the TOE are only needed for specified sub-environments. Because the TOE is intended to address a single “security criteria,” the reader can assume that all Policy and Threat statements apply to the “system” (SYS) partition, unless otherwise stated. Certain policies and threats apply only to the CS or the RU partition, and are labelled as such.

Travelling users and telecommuters are both treated as the “remote unit” in this profile. The travelling user will normally communicate with their home enclave from a physically unsecured facility/environment (e.g. hotel room, contractor office, airplane, etc.) using a portable, lightweight, client workstation. The travelling user may be accessing the home enclave during normal work hours, or after hours. However, remote access will typically be for a limited amount of time (i.e., not 24 hours per day access). The telecommuter requires a workstation that is operated from a static location on a fairly regular basis. The telecommuter typically works during normal work hours from home or another office facility that lacks direct connectivity to the enclave network. Their environments apparently differ greatly in the degree of physical exposure to the remote workstation when comparing, say, an international traveller to a local telecommuter. However, when taking into account the sensitivity of information to be protected by the TOE, the two environments can be characterised as roughly equal in terms of threat exposure.

The TN is entirely outside the control of the organisation, with the available controls being only what the TN owner voluntarily provides. User access is not controllable and the environment is assumed to be hostile. Because the TN is outside the scope of control for the organisation, no security requirements can be attributed to it. Thus, the RU and CS must provide the primary security functions for the TOE.

An enclave is defined as a system or set of systems within the span of control of a local security authority that has a limited number of external connections to a telecommunications network. The CS, as described earlier in the description of the TOE, sits within the enclave and is the primary means of access to the enclave network for a RU. The CS is physically protected with limited access to authorised individuals, and has an adequate administrative staff available.

3.1 Organisational Security Policies

The following policy statements are derived from the following references:

- DoD Chief Information Officer (CIO) Guidance and Policy Memorandum No. 6-8510 - Department of Defense Information Assurance.

- CJCSI 6510.01, "Information Assurance (IA) Implementation (IA Defense in Depth and Computer Network Defense (CND))"
- OMB Cir. No. A-130, Management of Federal Information Resources .

The determination of adequate policy coverage must take into account interpretations of subjective terms such as “eligible” and “adequate.” This interpretative aspect is addressed in the Rationale sections of the PP.

P.ACCOUNT User activity shall be monitored to the extent that sanctions can be applied when malfeasance occurs, and to ensure that system controls are properly applied.

P.BANNER The TOE will provide a banner to notify authorised and non-authorised users that they have entered a government computer system.

Application Note: Users will also receive a banner, provided by the local RU or the enclave system with which they are connecting.

P.CONFIDENTIALITY The TOE shall provide controls that are adequate to protect the confidentiality of user data being exchanged, TSF data, and access to the network.

P.ELGIBLE Authorised users and administrators of the TOE shall be eligible to access information that is created, communicated, processed, or stored on the TOE.

P.INTEGRITY The TOE will provide controls to protect access to, and the integrity of TOE resources.

P.MANAGE The TOE shall be managed such that its security functions are implemented and preserved throughout its operational lifetime.

P.PROCEDURES Procedures will be in place to restrict inadvertent disclosures or modification of sensitive information or improper utilisation of resources in the TSE.

P.REMOTE_ADMIN Authorised administrators may remotely administer devices in the TSE through protected external communication channels.

P.TRAINING All TOE users and administrators will be properly trained on the TSF prior to accessing an operational TOE.

3.1.1 CS Policy

The following security policy is specific to the CS:

P.EXPORT$_{(CS)}$ Authorised users and administrators of the TOE shall not export TSF data without proper and explicit authorisation.

3.1.2 RU Policy

The following security policy is specific to the RU:

P.AUTHENTICATE Authentication mechanisms for the remote unit will be maintained separate when not in use.

3.2 Threats to Security

The TOE must provide uniform protection against the threats outlined here. The determination of adequate threat mitigation is addressed in the Rationale sections of the PP.

The attacks outlined in the specified threats may be motivated by deliberate malice or could be the result of unintentional mistakes on behalf of the improperly trained user. Results of a deliberate attack can be especially damaging to the organisation's information system due to the attacker's advantage of knowing the network's configuration and thus its vulnerabilities.

The threats listed below are those that are addressed by a remote access system that is compliant with this Protection Profile. All the malicious threat agents may have high levels of expertise, resources, and motivation. The term "compromise" (when unqualified) refers to a degradation of the confidentiality and/or integrity of some asset.

T.ALTER An unauthorised user may surreptitiously gain access to the TOE and attempt to alter and/ or replace system elements (e.g. hardware, firmware, or software) in an attempt to subvert the device.

T.BACKUP Failure to adequately perform system backup of TSF data may result in compromise or system non-availability.

T.CAPTURE An agent may eavesdrop on, or otherwise capture, data being transferred on a communications channel.

T.CRYPTANALYTIC Unauthorised agents may passively attack the cryptography of the TOE using cryptanalysis methods.

T.DENIAL An unauthorised user may render the TOE unavailable for use.

T.ERROR A user may attempt to perform unauthorised or erroneous actions that will compromise user and/or system resources.

T.IMPORT An authorised user or administrator of the TOE may unwittingly introduce malicious code into the system, resulting in a compromise of the integrity and/or availability of system resources.

T.INTRUDE An unauthorised user may use the TOE to gain access to the secure enclave.

T.MASQUERADE An unauthorised user may attempt to gain access to the TOE by pretending to be an authorised user.

T.MEDIA Failure to adequately protect storage media may result in compromise or non-availability of the TOE.

T.MODIFY An unauthorised modification of the TSF data may occur.

T.PHYSICAL TOE security functions (TSF) may be subject to physical attack that may compromise security.

T.REPEAT An unauthorised user may repeatedly attempt to guess authentication information.

T.REPUDIATION Authorised users or administrators may deny originating or receiving data transfers or performing malicious acts.

T.TRAFFIC Use of the TOE may transmit (via traffic analysis or covert channel analysis) sensitive information to unauthorised users.

T.UNDETECT Compromises of user resources or system resources (by any threat agent) may go undetected for long periods of time.

3.2.1 CS Threats

The following security threats are specific to the CS:

T.AUDFAIL$_{(CS)}$ System modification, compromise, or full audit file may result in failure to collect audit data.

T.AUDREV(CS) Appropriate individuals may fail to adequately review and interpret the audit data, or take appropriate action.

3.3 Secure Usage Assumptions

The different threat environments that result from the operational characteristics of the TOE results in differing specifications of required assumptions. These assumptions are relative to partitions defined for the TOE.

3.3.1 CS Assumptions

The following security assumptions are specific to the CS:

A.LIM_ACCESS$_{(CS)}$ The CS is physically isolated so that only authorised personnel can physically access it.

3.3.2 Remote Unit Assumptions

The following security assumptions are specific to the RU:

A.TRUSTED_USER$_{(RU)}$ Authorised users of the RU will not intentionally violate organisational security policies.

A.PHYSICAL_SECURITY$_{(RU)}$ Physical security of the TSE at an RU site must be considered limited since remote sites are typically located in a higher threat environment.

3.3.3 System Assumptions

The following assumptions pertain to the overall Remote Access system TOE. Some of these assumptions can be made about the individual components of the RAS, but at a minimum are appropriate at the system level.

A.AVAILABLE Functional use of the TOE assumes that the telephone network is available.

A.BANNER$_{(SYS)}$ A banner to notify all users that they are entering a government computer system will be provided by the TOE.

A.CRYPTANALYTIC$_{(SYS)}$ Cryptographic methods used in the TOE will be resistant to cryptanalytic attacks and be of adequate strength to protect sensitive data.

A.CRYPTO_SUPPORT$_{(SYS)}$ Cryptographic support infrastructure will be provided by procedures and mechanisms external to the TOE.

A.TRUSTED_ADMIN$_{(SYS)}$ Administrators will not deliberately abuse their privileges so as to violate organisational security policies and are competent to manage the TOE and the information it contains, although they are capable of error.

4—Security Objectives

4.1 Security Objectives for the TOE

The following are the IT security objectives for the TOE. They are now partitioned along the same lines as the environment.

4.2 Security Objectives for the CS

O.DETECT$_{(CS)}$ The CS will detect unauthorised changes to RU configurations, when an RU connects to the CS.

O.AUDIT$_{(CS)}$ The TOE will provide an audit trail to ensure each authenticated user and TOE administrator can be held accountable for his or her actions in the TOE. The audit trail will be of sufficient detail to reconstruct events in determining the cause or magnitude of compromise should a security violation or malfunction occur.

O.CS_AVAILABLE$_{(CS)}$ The CS will not allow a single user identity to connect to more than one incoming modem port at one time.

4.2.1 Security Objectives for the RU

O.MEDIA$_{(RU)}$ The RU will protect sensitive data stored on it such that this data is unavailable while the TOE is not in use.

O.ACCESS$_{(RU)}$ During operation, the RU will limit access to system resources to authorised users.

4.2.2 Security Objectives for the SYS

O.ACCESS$_{(SYS)}$ The TOE will control access to information that is subject to the enclave security policy, based on the identity of the accountable individuals, such that this policy cannot be bypassed in the TOE.

O.ANTIVIRUS$_{(SYS)}$ The TOE will provide for effective malicious code detection and elimination.

O.BANNER$_{(SYS)}$ The TOE will provide a banner to notify all users that they are entering a government computer system.

O.CRYPTO_SUPPORT$_{(SYS)}$ The TOE must interface with cryptographic support mechanisms, that establish files and configuration parameters and ensures the integrity of these files and parameters.

O.IDENTIFY$_{(SYS)}$ The TOE will uniquely identify and authenticate individuals.

O.INTEGRITY$_{(SYS)}$ The TOE will apply integrity protection to all information transmitted between the RU and the CS.

O.MANAGE$_{\text{(SYS)}}$ The TOE will provide adequate management features for its security functions.

O.NO_EAVESDROP$_{\text{(SYS)}}$ The TOE will prevent, with a strength appropriate for tunnelling SBU data across a public network, the disclosure of information during transfers between an RU and the CS.

O.RECEIVE$_{\text{(SYS)}}$ A CS or a RU will only accept remote commands and data from another CS or RU with which it is mutually authenticated.

O.SECURE_STARTUP$_{\text{(SYS)}}$ Upon initial start-up of the TOE or recovery from an interruption in TOE services, the TOE must default to a secure state and not compromise its files, configuration parameters, or information being processed before the interruption occurred.

O.SELF_PROTECT$_{\text{(SYS)}}$ The TOE will protect its security-related functions against external interference or tampering by users, or attempts by users to bypass its security functions.

O.SELF_TEST$_{\text{(SYS)}}$ The TOE will perform self-tests of its security functions including those required by the site security policy and site procedures.

4.3 Security Objectives for the Environment

The following are the Protection Profile security objectives that will be satisfied largely through application of procedural or administrative measures.

OE.BACKUP$_{\text{(CS)}}$ Administrators will perform periodic backups to protect TSF data.

OE.INSTALL$_{\text{(SYS)}}$ Those responsible for the TOE must ensure the remote access system will be delivered, installed, and managed in a manner which maintains the system security.

OE.PHYSICAL$_{\text{(SYS)}}$ Those responsible for the TOE must ensure that TOE hardware, software, and documentation will be protected from unauthorised access, and all SBU data handled by the TOE will be protected to prevent unauthorised (intentional or unintentional) disclosure.

OE.REVIEW$_{\text{(CS)}}$ Administrators will periodically review audit trail information, and appropriate action should be taken on the detection of breaches of security, or events that are likely to lead to a breach in the future.

OE.TRAIN$_{\text{(SYS)}}$ Authorised users and administrators are trained to develop and administer security policies and practices.

5—IT Security Requirements

5.1 TOE Security Functional Requirements

5.1.1 Security Audit (FAU)

5.1.1.1 Security alarms (FAU_ARP.1$_{(SYS)}$)

The TSF shall take **an action to alert an administrator of the system** upon detection of a potential security violation. FAU_ARP.1.1

Application Note: The most relevant potential security violations that this requirement applies to include repeated login failure attempts and other system penetration activities. Superior implementations are those that support configurable actions for the events considered to be potential security violation. This includes a CS checking for unauthorised modifications on the Remote Unit.

5.1.1.2 Audit data generation (FAU_GEN.1$_{(CS)}$)

The TSF shall be able to generate an audit record of the following auditable events:

a) Start-up and shutdown of the audit functions;

b) All auditable events for the minimum level of audit, as shown in table 5-1; and

c) No other events. FAU_GEN.1.1

Table 5-1 FAU_GEN.1 Auditable Events

Component	Auditable Events
FAU_ARP.1	Actions taken due to imminent security violations.
FAU_SAA.1	Enabling and disabling of any of the analysis mechanisms.
FAU_SAA.3	Enabling and disabling of any of the analysis mechanisms.
FAU_SAR.1	Reading of information from the audit records.
FAU_SAR.2	Unsuccessful reading of information from the audit records.
FAU_SAR.3	The parameters used for viewing audit records.
FAU_STG.4	Actions taken due to audit storage failure.
FCO_NRO.2	The invocation of the non-repudiation service.
FCS_CKM.1	Success and failure of the activity.

Component	Auditable Events
FCS_CKM.2	Success and failure of the activity.
FCS.CKM.4	Success and failure of the activity.
FCS.COP.1	Success and failure and the type of cryptographic operation.
FDP_ACF.1	All requests to perform an operation on an object covered by the SFP.
FDP_IFF.1	Managing the attributes used to make explicit access based decisions.
FDP_ITT.1	All attempts to transfer user data, including the protection method used and any errors that occurred.
FDP_ITT.3	All attempts to transfer user data, including identification of the integrity protection method used and any errors that occurred.
FDP_SDI.2	All attempts to check the integrity of user data, including an indication of the results of the check, if performed.
FIA_AFL.1	The reaching of the threshold for the unsuccessful authentication attempts and the actions (e.g. disabling of a terminal) taken and the subsequent, if appropriate, restoration to the normal state (e.g. re-enabling of a terminal).
FIA_SOS.1	Rejection by the TSF of any tested secret.
FIA_SOS.2	Rejection by the TSF of any tested secret.
FIA_UAU.2.	All use of the authentication mechanism.
FIA_UAU.6	All reauthentication attempts.
FIA_UID.2	All use of the user identification mechanism, including the user identity provided.
FIA_USB.1	Success and failure of binding of user security attributes to a subject (e.g. success and failure to create a subject).
FMT_MOF.1	All modifications in the behaviour of the functions in the TSF.
FMT_MSA.1	All modifications of the values of security attributes
FMT_MSA.2	All offered and accepted secure values for a security attribute
FMT_MSA.3	Modifications of the default setting of permissive or restrictive rules. All modifications of the initial values of security attributes
FMT_MTD.1	All modifications to the values of TSF data.
FMT_REV.1	All attempts to revoke security attributes.

Component	Auditable Events
FMT_SAE.1	Specification of the expiration time for an attribute. Action taken due to attribute expiration.
FMT_SMR.1	Modifications to the group of users that are part of a role.
FPT_ITT.3	The detection of modification of TSF data.
FPT_RPL.1	Action to be taken based on the specific actions
FPT_STM.1	Minimal changes to the time.
FRU_RSA.1	Rejection of allocation operation due to resource limits.

The TSF shall record within each audit record at least the following information:

a) Date and time of the event, type of event, subject identity, and the outcome (success or failure) of the event; and

b) For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, **a session identifier and** [*ST assignment: other audit relevant information].* FAU_GEN.1.2

Application Note: FAU_GEN.1 does not list auditable event requirements (see Table FAU_GEN.1.1) for functional components associated with the RU partition. The RU partition does not include an audit generation capability and so those functional components cannot generate audit records. Similarly, those auditable event requirements that apply to the SYS partition should be interpreted as applying only to the CS partition. FAU_GEN.1.1 lists specific audit requirements associated with functional components included in the profile, excluding the RU-specific functional components. FAU_GEN.1.2, without modification, specifies most of the audit data required to address accountability concerns. The success or failure of events may sometimes be an implicit property of an audit record. This element adds “session identifier” to complement the intrinsically defined audit data requirements. Furthermore, this is an extensible element and allows the ST author to provide additional audit data detail.

5.1.1.3 User identity association (FAU_GEN.2$_{(CS)}$)

The TSF shall be able to associate each auditable event with the identity of the user that caused the event. FAU_GEN.2.1

Application Note: Before remote users are authenticated, there may be audit data that is of security relevance. For instance, the CS may record a lot of audit data associated with an intrusion attempt without ever being able to identify a valid user. In these cases, it is acceptable that pseudo identities be used, as long as activities can be associated with unique entities. It should be possible to associate these activities with a specific user if that user successfully completes I&A.

5.1.1.4 Potential violation analysis (FAU_SAA.1$_{(CS)}$)

The TSF shall be able to apply a set of rules in monitoring the audited events and based upon these rules indicate a potential violation of the TSP. FAU_SAA.1.1

The TSF shall enforce the following rules for monitoring audited events:

a) Accumulation or combination of *[ST assignment: subset of defined auditable events]* known to indicate a potential security violation;

b) [ST assignment: any other rules]. FAU_SAA.1.2

5.1.1.5 Simple attack heuristics (FAU_SAA.3$_{(SYS)}$)

The TSF shall be able to maintain an internal representation of the following signature events: **unauthorised modifications to RU configuration data** that may indicate a violation of the TSP. FAU_SAA.3.1

The TSF shall be able to compare the signature events against the record of system activity discernible from an examination of **configuration data.** FAU_SAA.3.2

The TSF shall be able to indicate an imminent violation of the TSP when a system event is found to match a signature event that indicates a potential violation of the TSP. FAU_SAA.3.3

Application Note: The internal representation that is maintained by the TSF need not be generated at the same time the signature event occurs. However, the internal representation must be generated before the configuration data is used again. The CS will verify the configuration of the RU when an RU attempts to connect to the CS. An allowed configuration will be maintained by the CS as a reference.

5.1.1.6 Audit review (FAU_SAR.1$_{(CS)}$)

The TSF shall provide **administrators** with the capability to read **all data** from the audit records. FAU_SAR.1.1

The TSF shall provide the audit records in a manner suitable for the user to interpret the information. FAU_SAR.1.2

Application Note: Administrators should have the capability to access all audit data.

5.1.1.7 Restricted audit review (FAU_SAR.2$_{(CS)}$)

The TSF shall prohibit non-administrators read access to the audit records, except those users that have been granted explicit read-access. FAU_SAR.2.1

Application Note: Some applications may allow or require some users to read audit records. However, in those cases, access must be explicit and available mechanisms and/ or procedures must guarantee the proper granularity of access to audit data.

5.1.1.8 Selectable audit review (FAU_SAR.3$_{(CS)}$)

The TSF shall provide the ability to perform searches, sorting, and ordering of audit data based on **date and time of the event, type of event, user identity, event success or failure criteria, and session identifier.** FAU_SAR.3.1

Application Note: The selection criteria exactly mirrors the data that FAU_GEN.1.2 requires to be in every record. Here we require review operations on the basis of user (rather than subject) identity, to indicate that some method must exist within the audit review mechanism to associate audit data attributed to subjects to unique individuals.

5.1.1.9 Guarantees of audit data availability (FAU_STG.2$_{(CS)}$)

The TSF shall protect the stored audit records from unauthorised deletion. FAU_STG.2.1

The TSF shall be able to prevent modifications to the audit records. FAU_STG.2.2

The TSF shall ensure that **the most recent 24 hours of** audit records will be maintained when the following conditions occur: audit storage exhaustion, failure or attack. FAU_STG.2.3

5.1.1.10 Prevention of audit data loss (FAU_STG.4$_{(CS)}$)

The TSF shall *[ST selection: 'prevent auditable events,' 'overwrite the oldest stored audit records']* and *[ST assignment: other actions to be taken in case of audit storage failure]* if the audit trail is full. FAU_STG.4.1

Application Note: It is important that if overwriting the audit trail is implemented for the TOE, the period between audit trail overwrites be long enough to allow for necessary audit review tasks and/or off-loading of audit data (if desired). This is an expected responsibility of the administrator and some type of note should be sent to the user to alert them that the audit trail is full.

5.1.2 Communication (FCO)

5.1.2.1 Enforced Proof of Origin (FCO_NRO.2)

The TSF shall enforce the generation of evidence for transmitted **Remote User's data transfers, System & Security Administrator's commands, TOE to TOE transmissions** at all times. $^{\text{FCO\_NRO.2.1}}$

The TSF shall be able to relate the **Remote User's identity, System & Security Administrator's identity, identity of transmitting TOE** of the originator of the information, and the **datagram content** of the information to which the evidence applies. $^{\text{FCO\_NRO.2.2}}$

The TSF shall provide a capability to verify the evidence of origin of information to *CS* given **immediate verification**. $^{\text{FCO\_NRO.2.3}}$

5.1.3 Cryptographic Support (FCS)

5.1.3.1 Cryptographic Key Generation (FCS_CKM.1$_{\text{(SYS)}}$)

The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm *[ST assignment: Type 2 cryptographic key generation algorithm]* and specified cryptographic key sizes *[ST assignment: Type 2 cryptographic key sizes]* that meet the following: *[ST assignment: Type 2 cryptographic standards]*. $^{\text{FCS\_CKM.1.1}}$

Application Note: For this requirement, all ST assignments should follow national policies and directives relative to the protection of SBU information.

5.1.3.2 Cryptographic Key Distribution (FCS_CKM.2$_{\text{(SYS)}}$)

The TSF shall distribute cryptographic keys in accordance with a specified cryptographic key distribution method *[ST assignment: Type 2 cryptographic key distribution method].* $^{\text{FCS\_CKM.2.1}}$

Application Note: For this requirement, all ST assignments should follow national policies and directives relative to the protection of SBU information.

5.1.3.3 Cryptographic Key Destruction (FCS_CKM.4$_{\text{(SYS)}}$)

The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction methods *[ST assignment: Type 2 cryptographic key destruction method]* that meets the following: *[ST assignment: Type 2 list of standards]*. $^{\text{FCS\_CKM.4.1}}$

Application Note: For this requirement, all ST assignments should follow national policies and directives relative to the protection of SBU information.

5.1.3.4 Cryptographic Operation (FCS_COP.1$_{(CS)}$)

The TSF shall perform

a) CS to RU authentication, and

b) **encryption of user data during transmission to the RU**,

in accordance with a specified cryptographic algorithm [ST *assignment: Type 2 cryptographic algorithm*] and cryptographic key sizes [ST assignment: *Type 2 cryptographic key sizes*] that meet the following: *[ST assignment: Type 2 list of standards]*. FCS_COP.1.1

Application Note: For this requirement, all ST assignments should follow national policies and directives relative to the protection of SBU information.

5.1.3.5 Cryptographic Operation (FCS_COP.1$_{(RU)}$)

The TSF shall perform

a) RU to CS authentication,

b) encryption of user data during transmission to the CS,

c) cryptographic checksum on RU configuration data, and

d) **encryption of user data on the RU,**

in accordance with a specified cryptographic algorithm *[ST assignment: Type 2 cryptographic algorithm]* and cryptographic key sizes *[ST assignment: Type 2 cryptographic key sizes]* that meet the following: *[ST assignment: Type 2 list of standards]*. FCS_COP.1.1

Application Note: For this requirement, all ST assignments should follow national policies and directives relative to the protection of SBU information. All stored data will be encrypted using Type 2 cryptographic algorithms.

5.1.4 User Data Protection (FDP)

5.1.4.1 Subset access control (FDP_ACC.1$_{(RU)}$)

The TSF shall enforce the **policy P.RU_ACCESS (User access to the RU terminal will be granted to authorised users based on proper authentication and permissions)** on **the users** and operations among subjects covered by the SFP. FDP_ACC.1.1

Application note: As a minimum the TSF must enforce these specific policies. The RAS will have a system security policy (see ADV_SPM.1), which must be enforced by the TSF. P.RU_ACCESS should be included as part of the RAS security policy.

5.1.4.2 Subset access control (FDP_ACC.$1_{(SYS)}$)

The TSF shall enforce the **policy P.ADMIN_ACCESS (Only administrators have access to view and/or modify TOE security functions.)** on **the administrator** and operations among subjects covered by the SFP. FDP_ACC.1.1

Application Note: As used in this context, subjects are envisioned to be administrators, and TOE security functions are considered objects. As a minimum the TSF must enforce these specific policies. The RAS will have a system security policy (see ADV_SPM.1), which must be enforced by the TSF. P.ADMIN_ACCESS should be included as part of the RAS security policy.

5.1.4.3 Security attribute based access control (FDP_ACF.1)

The TSF shall enforce the policy **P.USER_ACCESS (Access to the secure network through the CS will be granted to the user based on proper authentication and permissions.)** to objects based on **attributes of an administrator group or user groups**. FDP_ACF.1.1(SYS)

The TSF shall enforce the policies **P.RU_ACCESS** and **P.USER_ACCESS** to objects based on **attributes of user groups**. FDP_ACF.1.1(RU)

The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed:

a) **TOE access is granted to administrators with read, write, and modify permissions**,

b) TOE access is granted to users based on group permissions.FDP_ACF.1.2

The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: **none**. FDP_ACF.1.3

The TSF shall explicitly deny access of subjects to objects based on the **policy P.USER_ACCESS**. FDP_ACF.1.4

Application note: As a minimum the TSF must enforce these specific policies. The RAS will have a system security policy (see ADV_SPM.1), which must be enforced by the TSF. P.USER_ACCESS should be included as part of the RAS security policy.

5.1.4.4 Stored data integrity monitoring and action (FDP_SDI.2)

The TSF shall monitor user data stored within the RU for integrity error in configuration data, based on the following attributes: [***ST assignment: standard configuration setup***]. FDP_SDI.2.1

Upon detection of a data integrity error, the TSF shall **take an alarm action to alert authorised users of the RU**. FDP_SDI.2.2

5.1.4.5 Subset information flow control. (FDP_IFC.1$_{(CS)}$)

The TSF shall enforce the **P.SEPARATE (User data may only flow within the CS between an RU connection and the associated enclave session.) policy** on **user data**. FDP_IFC.1.1

Application Note: As a minimum the TSF must enforce these specific policies. The RAS will have a system security policy (see ADV_SPM.1), which must be enforced by the TSF. P.SEPARATE should be included as part of the RAS security policy.

5.1.4.6 Subset information flow control. (FDP_IFC.1$_{(SYS)}$)

The TSF shall enforce the **P.RECEIVE (A RU will only accept remote information from the CS with which it is authenticated, and the TOE CS will only accept remote information from an authenticated RU.) policy** on **all TN communications, RU and CS**. FDP_IFC.1.1

Application Note: As a minimum the TSF must enforce these specific policies. The RAS will have a system security policy (see ADV_SPM.1), which must be enforced by the TSF. P.RECEIVE should be included as part of the RAS security policy.

5.1.4.7 Simple security attributes. (FDP_IFF.1$_{(CS)}$)

The TSF shall enforce the **P.SEPARATE policy** based on the following types of subject and information security attributes**: remote user identity and enclave session identity**. FDP_IFF.1.1

The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold: **the remote user identity and the enclave session identity of the subject match that of user data that it accesses**. FDP_IFF.1.2

The TSF shall enforce: **the remote user identity of a subject corresponds to the user identity of the enclave session identified by the subject's enclave session identity attribute**. FDP_IFF.1.3

The TSF shall provide the following: **no additional SFP capabilities**. FDP_IFF.1.4

The TSF shall explicitly authorise an information flow based on the following rules: **none**. FDP_IFF.1.5

The TSF shall explicitly deny an information flow based on the following rules: **none**. FDP_IFF.1.6

Application Note: The only requirement is to control information flow in the CS based on remote user and session identities.

5.1.4.8 Simple security attributes. (FDP_IFF.1$_{(SYS)}$)

The TSF shall enforce the **P.RECEIVE policy** based on the following types of subject and information security attributes: **remote user identity**. FDP_IFF.1.1

The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold: **the remote user identity is authenticated with the CS.** FDP_IFF.1.2

The TSF shall enforce: **no additional information control SFP rules.** FDP_IFF.1.3

The TSF shall provide the following: **no additional SFP capabilities.** FDP_IFF.1.4

The TSF shall explicitly authorise an information flow based on the following rules: **none.** FDP_IFF.1.5

The TSF shall explicitly deny an information flow based on the following rules: **none.** FDP_IFF.1.6

5.1.4.9 Basic internal transfer protection (FDP_ITT.1$_{(SYS)}$)

The TSF shall enforce the **P.RECEIVE policy** to prevent the <u>disclosure or modification</u> of user data when it is transmitted between physically separated parts of the TOE. FDP_ITT.1.1.

Application Note: This is translated into FDP_UCT.1 for the RU and the CS when the TOE is decomposed. It relies on FCS_COP.1.

5.1.4.10 Integrity monitoring (FDP_ITT.3$_{(SYS)}$)

The TSF shall enforce the **P.RECEIVE policy** to monitor user data transmitted between physically separated parts of the TOE for the following errors: **modification of data, substitution of data, replay of data, and deletion of data.** FDP_ITT.3.1

Upon detection of a data integrity error, the TSF shall **discard the affected data.** FDP_ITT.3.2

Application Note: This is translated into FDP_UIT.1 for the RU and the CS when the TOE is decomposed. It relies on FCS_COP.1.

5.1.4.11 Full residual information protection. (FDP_RIP.2$_{(RU)}$)

The TSF shall ensure that any previous information content of a resource is made unavailable upon the deallocation of the resource from all objects. FDP_RIP.2.1.

Application Note: The resources include data storage and communication channels when deallocated from SBU processing. It relies on FCS_COP.1.

5.1.5 Identification and Authentication (FIA)

Requirements Overview: The intention of the next two components is that the CS should lock a user account that experiences repeated unsuccessful authentication attempts and, similarly, an RU should be locked if a user makes repeated failed attempts to authenticate to the RU.

5.1.5.1 Authentication failure handling (FIA_AFL.1$_{(CS)}$)

The TSF shall detect when **an administrator-configurable number** unsuccessful authentication attempts occur related to **cumulative authentication failures of a specific user identity to a CS.** FIA_AFL.1.1

When the defined number of unsuccessful authentication attempts has been met or surpassed, the TSF shall **lock the user account on the CS.** FIA_AFL.1.2

Application Note: FIA_AFL.1.1 refers to the total number of consecutive failed authentication attempts for a specific, valid user identity to the CS. The user should be locked out until an administrator reconfigures the CS. The defined number of unsuccessful authentication attempts should be a positive integer.

5.1.5.2 Authentication failure handling (FIA_AFL.1$_{(RU)}$)

The TSF shall detect when **an administrator-configurable number** unsuccessful authentication attempts occur related to **cumulative authentication failures of a specific user identity to an RU.** FIA_AFL.1.1

When the defined number of unsuccessful authentication attempts has been met or surpassed, the TSF shall **lock the user account on that RU.** FIA_AFL.1.2

Application Note: FIA_AFL.1.1 refers to the total number of consecutive failed authentication attempts for a specific, valid user identity to a RU. The user should be locked out until an administrator reconfigures the RU. The defined number of unsuccessful authentication attempts should be a positive integer.

5.1.5.3 User Attribute Definition (FIA_ATD.1$_{(SYS)}$)

The TSF shall maintain the following list of security attributes belonging to individual users: **remote user identities and enclave session identifiers.** FIA_ATD.1.1

5.1.5.4 Verification of Secrets (FIA_SOS.1$_{(SYS)}$)

The TSF shall provide a mechanism to verify that secrets meet **an appropriate bit length in accordance with specified algorithm and key length, and not key that is all ones, all zeros, or repeating patterns**. FIA_SOS.1.1

5.1.5.5 TSF Generation of Secrets (FIA_SOS.2$_{(SYS)}$)

The TSF shall provide a mechanism to generate secrets that meet **an appropriate bit length in accordance with specified algorithm and key length, and not key that is all ones, all zeros, or repeating patterns**. FIA_SOS.2.1

The TSF shall be able to enforce the use of TSF generated secrets for **unique RU-to-CS session keys.** FIA_SOS.2.2

5.1.5.6 User authentication before any action (FIA_UAU.2$_{(SYS)}$)

The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user. FIA_UAU.2.1

Application Note: Network traffic that flows through a CS to an RU partition shall be considered to be performed on behalf of the user at the RU.

5.1.5.7 Re-authenticating (FIA_UAU.6$_{(RU)}$)

The TSF shall re-authenticate the user under the conditions **when TSF-initiated session locking is triggered.** FIA_UAU.6.1

Application Note: See requirement FTA_SSL.1$_{(RU)}$ as a reference for TSF-initiated session locking.

5.1.5.8 Re-authenticating (FIA_UAU.6$_{(CS)}$)

The TSF shall re-authenticate the administrator under the conditions **when TSF-initiated session locking is triggered.** FIA_UAU.6.1

Application Note: See requirement FTA_SSL.1$_{(CS)}$ as a reference for TSF-initiated session locking.

5.1.5.9 Protected authentication feedback (FIA_UAU.7$_{(SYS)}$)

The TSF shall provide only **acknowledgement of data entry** to the user while the authentication is in progress. FIA_UAU.7.1

Application Note: The authentication data that is provided by direct user entry shall not be displayed. In particular, if the user is required to enter a PIN at a keyboard for smartcard authentication, then the PIN should not be displayed, but it would be acceptable (desirable) to display a positive acknowledgement of each keystroke.

5.1.5.10 User Identification before any action (FIA_UID.2$_{(SYS)}$)

The TSF shall require each user to identify itself before allowing any other TSF-mediated actions on behalf of that user. FIA_UID.2.1

Application Note: The user must authenticate to the RU before retrieving data or connecting to the CS.

5.1.5.11 User-Subject Binding (FIA_USB.1$_{(CS)}$)

The TSF shall associate the appropriate user security attributes with subjects acting on behalf of that user. FIA_USB.1.1

Application Note: The only attributes that we have explicitly identified are the user identity and session identifier.

5.1.6 Security Management (FMT)

5.1.6.1 Management of security functions behaviour (FMT_MOF.1$_{(SYS)}$)

The TSF shall restrict the ability to determine and modify the behaviour of the functions **listed in Table 5-2. FMT_MOF.1; Managed Security Functions** to **an administrator role.** FMT_MOF.1.1

Table 5-2. FMT_MOF.1; Managed Security Functions

Component	Management Function
FAU_ARP.1$_{(CS)}$ FAU_ARP.1$_{(RU)}$	The addition, removal, or modification of alarms.
FAU_SAA.1$_{(CS)}$	Adding, modifying, or deletion of rules from the set of rules.
FAU_SAA.3$_{(RU)}$	Deleting, modifying, or adding signature events.
FAU_SAR.1$_{(CS)}$	Deleting, modifying, or adding users with read access right to the audit records.
FAU_STG.4$_{(CS)}$	Deleting, modifying, or adding actions to be taken in case of audit storage failure.
FCS_CKM.1$_{(SYS)}$ FCS_CKM.3$_{(SYS)}$ FCS_CKM.4$_{(SYS)}$	The management of changes to cryptographic key attributes. Examples of key attributes include user, key type (e.g. public, private, secret), validity period, and use (e.g. digital signature, key encryption, key agreement, data encryption).
FDP_IFF.1$_{(CS)}$ FDP_IFF.1$_{(SYS)}$	Managing the attributes used to make explicit access based decisions.
FDP_ITT.3$_{(SYS)}$	N/A: These are hard-wired functions.
FDP_RIP.2$_{(MU)}$	Performing residual information protection of the RU within the secure enclave.
FIA_AFL.1$_{(CS)}$ FIA_AFL.1$_{(RU)}$	Management of the threshold for unsuccessful authentication attempts. Management of locking and unlocking user accounts.
FIA_UAU.2$_{(SYS)}$	Management of the authentication data.
FIA_UID.2$_{(SYS)}$	The management of the user identities.
FIA_USB.1$_{(SYS)}$	Definition of default subject security attributes.
FMT_REV.1$_{(SYS)}$	(see FIA_UID.2)
FMT_SAE.1$_{(CS)}$	The management of actions to be taken if the expiration time has passed.
FMT_SMR.1$_{(SYS)}$	Managing the groups of individuals that are authorised users and/or administrators.
FPT_ITT.2$_{(SYS)}$	Management of the mechanism used to provide the protection of the data in transit between different parts of the TSF. Management of the separation mechanism.

Component	Management Function
FPT_ITT.3$_{(SYS)}$	Management of the types of modification against which the TSF should protect. Management of the mechanism used to provide the protection of the data in transit between different parts of the TSF.
FPT_STM.1$_{(CS)}$	Management of the time.
FPT_SSL.1$_{(RU) \& (CS)}$	Specification of the time of user inactivity after which lock-out occurs. Specification of the default time of user inactivity after which lock-out occurs. Management of the events that should occur prior to unlocking the session.
FTA_TAB.1$_{(SYS)}$	Maintenance of the banner by the administrator.

5.1.6.2 Management of security functions behaviour (FMT_MOF.1$_{(RU)}$)

The TSF shall restrict the ability to **determine and modify the behaviour of** the functions **listed in Table 5-2. FMT_MOF.1; Managed Security Functions** to **an administrator role.** FMT_MOF.1.1

Application Note: Table 5-2. FMT_MOF.1; Managed Security Functions lists security management functions that are explicitly required by this component. A combination of mechanisms (e.g., access controls and/or automated support tools) may be implemented to provide the capabilities called for in this component.

5.1.6.3 Management of security attributes (FMT_MSA.1$_{(SYS)}$)

The TSF shall enforce the **policy P.ADMIN_ACCESS** to restrict the ability to change_default, query, modify, or delete the security attributes **of user identity and session identifiers** to **administrators.** FMT_MSA.1.1

5.1.6.4 Secure security attributes (FMT_MSA.2$_{(SYS)}$)

The TSF shall ensure that only secure values are accepted for security attributes. FMT_MSA.2.1

5.1.6.5 Static attribute initialisation (FMT_MSA.3$_{(SYS)}$)

The TSF shall enforce the policy **P.ADMIN_ACCESS** to provide restrictive default values for security attributes that are used to enforce the SFP. FMT_MSA.3.1

The TSF shall allow the **administrator** to specify alternative initial values to override the default values when an object or information is created. FMT_MSA.3.2

5.1.6.6 Management of TSF data (FMT_MTD.1$_{(SYS)}$)

The TSF shall restrict the ability to change_default, query, modify, delete, or clear the

a) specification of user identities,

b) specification of valid RU-to-CS connections,

c) specification of valid CU-to-RU connections,

d) **specification of authorised RU peripheral devices, and**

e) [ST assignment: list of other TSF data]
to **administrators.** FMT_MTD.1.1

Application Note: All operations on TSF data is restricted to system administrators. Authorised users will have a defined user identity, that could be defined in varied implementations (e.g., a list of certificates or in a database). The specifications of TSF data listed are the minimum set. The list indicates what specifications of TSF data must be controlled to support the P.RECEIVE and P.SEPARATE or other Access Control policies.

5.1.6.7 Revocation (FMT_REV.1$_{(SYS)}$)

The TSF shall restrict the ability to revoke security attributes associated with the users within the TSC to **administrators.** FMT_REV.1.1

The TSF shall enforce the rules **immediate revocation of user identities and *[ST assignment: other revocation rules].*** FMT_REV.1.2

Application Note: A minimal implementation mechanism must provide an "immediate" revocation function. Subsequent attempts to access the TOE by a revoked identity should fail. Other, flexible revocation functions (e.g., immediate session termination) may also be desirable, depending upon the end user's needs.

5.1.6.8 Time-limited authorisation (FMT_SAE.1$_{(CS)}$)

The TSF shall restrict the capability to specify an expiration time for **user identities** to **administrators.** FMT_SAE.1.1

For each of these security attributes, the TSF shall be able to **deny TOE access** after the expiration time for the indicated security attribute has passed. FMT_SAE.1.2

Application Note: User identities may be based on a complex representation (e.g., cryptographic certificates) within the system. The only required capability is to deny access to the TOE for users with expired identities.

5.1.6.9 Security roles (FMT_SMR.1$_{(SYS)}$)

The TSF shall maintain the role **of administrator.** FMT_SMR.1.1

The TSF shall be able to associate users with roles. FMT_SMR.1.2

Application Note: Other role definitions are desirable but are not required. In some cases it will be appropriate for administrators to be users of the system, but it should be easy to distinguish when they are acting as administrators from when they are acting as authorised users. Administrators may access the CS via direct connection, via remote access from an RU, or via remote access from the back-side network.

5.1.7 Protection of TOE Security Functions (FPT)

5.1.7.1 Abstract machine testing (FPT_AMT.1$_{(SYS)}$)

The TSF shall run a suite of tests during initial start-up, periodically during normal operation, at the request of an authorised Administrator to demonstrate the correct operation of the security assumptions provided by the abstract machine that underlies the TSF. FPT_AMT.1.1

5.1.7.2 TSF data transfer separation (FPT_ITT.2$_{(SYS)}$)

The TSF shall protect TSF data from disclosure when it is transmitted between separate parts of the TOE. FPT_ITT.2.1.

The TSF shall separate user data from TSF data when such data is transmitted between separate parts of the TOE. FPT_ITT.2.2.

Application Note: This is translated into FPT_ITC.1 when the TOE is decomposed.

5.1.7.3 TSF data integrity monitoring (FPT_ITT.3$_{(SYS)}$)

The TSF shall be able to detect modification of data, substitution of data, and deletion of data for TSF data transmitted between separate parts of the TOE. FPT_ITT.3.1.

Upon detection of a data integrity error, the TSF shall take the following actions: **discard the affected data.** FPT_ITT.3.2.

Application Note: This is translated into FPT_ITI.1 when the TOE is decomposed.

5.1.7.4 Automated recovery (FPT_RCV.2$_{(SYS)}$)

When automated recovery from a failure or service discontinuity is not possible, the TSF shall enter a maintenance mode where the ability to return the TOE to a secure state is provided. FPT_RCV.2.1

For **power failures and loss of bit count integrity** the TSF shall ensure the return of the TOE to a secure state using automated procedures. FPT_RCV.2.2

5.1.7.5 Replay detection (FPT_RPL.1$_{(SYS)}$)

The TSF shall detect replay for the following entities: **messages sent between the RU and the CS.** FPT_RPL.1.1.

The TSF shall perform **deletion of repeated messages** when replay is detected. FPT_RPL.1.2.

5.1.7.6 Non-bypassability of the TSP (FPT_RVM.1$_{(SYS)}$)

The TSF shall ensure that TSP enforcement functions are invoked and succeed before each function within the TSC is allowed to proceed. FPT_RVM.1.1

5.1.7.7 TSF domain separation (FPT_SEP.1$_{(SYS)}$)

The TSF shall maintain a security domain for its own execution that protects it from interference and tampering by untrusted subjects. FPT_SEP.1.1.

The TSF shall enforce separation between the security domains of subjects in the TSC. FPT_SEP.1.2.

5.1.7.8 Reliable time stamps (FPT_STM.1$_{(CS)}$)

The TSF shall be able to provide reliable time stamps for its own use. FPT_STM.1.1

Application Note: The time stamp mechanism may be integrated with the audit generation mechanism.

5.1.7.9 TSF testing (FPT_TST.1)

The TSF shall run a suite of self tests during initial start-up, periodically during normal operation, at the request of the System or Security Administrators to demonstrate the correct operation of the TSF. FPT_TST.1.1

The TSF shall provide authorised **System and Security Administrators** with the capability to verify the integrity of TSF data. FPT_TST.1.2

The TSF shall provide authorised **System and Security Administrators** with the capability to verify the integrity of stored TSF executable code. FPT_TST.1.3

5.1.8 Resource Utilisation (FRU)

5.1.8.1 Maximum quotas (FRU_RSA.1$_{(CS)}$)

The TSF shall enforce maximum quotas of the following resources: **CS modem ports** that an individual remote user can use over a specified period of time. FRU_RSA.1.1

Application Note: A single remote user shall not be allowed to dial in to more than one modem port on the communications server at a time. Multiple simultaneous sessions attempting to use the same identity can indicate a spoofed user identity.

5.1.9 TOE Access (FTA)

5.1.9.1 TSF-initiated session locking (RU) (FTA_SSL.1$_{(RU)}$)

The TSF shall lock an interactive session after **an administrator-configurable time interval** by:

a) clearing or overwriting display devices, making the current contents unreadable;

b) disabling any activity of the user’s data access/display devices other than unlocking the session. FTA_SSL.1.1

The TSF shall require the following events to occur prior to unlocking the session: **re-authentication of the user to the RU** FTA_SSL.1.2 **.**

Application Note: The administrator should configure time intervals for inactivity time-outs based on considerations of risk versus mission criticality. Time-outs may be different for each RU in the system. The ST author should carefully define what constitutes “inactivity” for the TOE. For instance, remote users may be active on the RU while no data is being sent to the CS. Depending upon implementation choices and functional trade-offs, this scenario could be reasonably described as either an active, or inactive, user. It is important that the ST defines exactly what situations will cause session locking. In general, it is preferable for user inactivity to be closely associated with inactivity of the remote user at the RU (i.e., higher-level protocols on the RU).

5.1.9.2 TSF-initiated session locking (CS) (FTA_SSL.1$_{(CS)}$)

The TSF shall lock an interactive session after **an administrator-configurable time interval** by:

c) clearing or overwriting display devices, making the current contents unreadable;

d) disabling any activity of the user’s data access/display devices other than unlocking the session. FTA_SSL.1.1

The TSF shall require the following events to occur prior to unlocking the session: **re-authentication of the administrator to the CS.** FTA_SSL.1.2

Application Note: The administrator should configure time intervals for inactivity time-outs based on considerations of risk versus mission criticality. Administrator access to the CS is for performing administrator functions. Lengthy periods of inactivity are not likely in this case. The ST author should decide what is a reasonable amount of time for administrator inactivity.

5.1.9.3 Default TOE access banners (FTA_TAB.1$_{(SYS)}$)

Before establishing a user session, the TSF shall display an advisory warning message regarding unauthorised use of the TOE. FTA_TAB.1.1

Application Note: The contents of the advisory warning message should be configurable by the administrator.

5.2 TOE Security Assurance Requirements

The assurance requirements for the SBU Remote Access System are found in EAL 2, augmented with ADV_SPM.1 Informal TOE security policy model.

Table 5-3. Assurance Requirements for the TOE: EAL 2

Assurance Class	Assurance Components
Configuration Management	Configuration items ACM_CAP.2
Delivery and Operations	Delivery procedures ADO_DEL.1 Installation, generation, and start-up procedures ADO_IGS.1
Development	Informal functional specification ADV_FSP.1 Descriptive high-level design ADV_HLD.1 Informal correspondence demonstration ADV_RCR.1 Informal TOE security policy model. ADV_SPM.1
Guidance documents	Administrator guidance AGD_ADM.1 User guidance AGD_USR.1
Tests	Evidence of coverage ATE_COV.1 Functional testing ATE_FUN.1 Independent testing – sample ATE_IND.2
Vulnerability Assessment	Strength of TOE security function evaluation AVA_SOF.1 Developer vulnerability analysis AVA_VLA.1

5.2.1 Configuration Management

5.2.1.1 Configuration items (ACM_CAP.2)

The developer shall provide a reference for the TOE. ACM_CAP.2.1D

The developer shall use a CM system. ACM_CAP.2.2D

The developer shall provide CM documentation. ACM_CAP.2.3D

The reference for the TOE shall be unique to each version of the TOE. ACM_CAP.2.1C

The TOE shall be labelled with its reference. ACM_CAP.2.2C

The CM documentation shall include a configuration list. ACM_CAP.2.3C

The configuration list shall describe the configuration items that comprise the TOE. ACM_CAP.2.4C

The CM documentation shall describe the method used to uniquely identify the configuration items. ACM_CAP.2.5C

The CM system shall uniquely identify all configuration items. ACM_CAP.2.6C

The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence. ACM_CAP.2.1E

5.2.2 Delivery and Operation

5.2.2.1 Delivery procedures (ADO_DEL.1)

The developer shall document procedures for delivery of the TOE or parts of it to the user. ADO_DEL.1.1D

The developer shall use the delivery procedures. ADO_DEL.1.2D

The delivery documentation shall describe all procedures that are necessary to maintain security when distributing versions of the TOE to a user’s site. ADO_DEL.1.1C

The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence. ADO_DEL.1.1E

5.2.2.2 Installation, generation, and start-up procedures (ADO_IGS.1)

The developer shall document procedures necessary for the secure installation, generation, and start-up of the TOE. ADO_IGS.1.1D

The documentation shall describe the steps necessary for secure installation, generation, and start-up of the TOE. ADO_IGS.1.1C

The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence. ADO_IGS.1.1E

The evaluator shall determine that the installation, generation, and start-up procedures result in a secure configuration. ADO_IGS.1.2E

5.2.3 Development

5.2.3.1 Informal functional specification (ADV_FSP.1)

The developer shall provide a functional specification. ADV_FSP.1.1D

The functional specification shall describe the TSF and its external interfaces using an informal style. ADV_FSP.1.1C

The functional specification shall be internally consistent. ADV_FSP.1.2C

The functional specification shall describe the purpose and method of use of all external TSF interfaces, providing details of effects, exceptions and error messages, as appropriate. ADV_FSP.1.3C

The functional specification shall completely represent the TSF. ADV_FSP.1.4C

The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence. ADV_FSP.1.1E

The evaluator shall determine that the functional specification is an accurate and complete instantiation of the TOE security functional requirements. ADV_FSP.1.2E

5.2.3.2 Descriptive high-level design (ADV_HLD.1)

The developer shall provide the high-level design of the TSF. ADV_HLD.1.1D

The presentation of the high-level design shall be informal. ADV_HLD.1.1C

The high-level design shall be internally consistent. ADV_HLD.1.2C

The high-level design shall describe the structure of the TSF in terms of subsystems. ADV_HLD.1.3C

The high-level design shall describe the security functionality provided by each subsystem of the TSF. ADV_HLD.1.4C

The high-level design shall identify any underlying hardware, firmware, and/or software required by the TSF with a presentation of the functions provided by the supporting protection mechanisms implemented in that hardware, firmware, or software. ADV_HLD.1.5C

The high-level design shall identify all interfaces to the subsystems of the TSF. ADV_HLD.1.6C

The high-level design shall identify which of the interfaces to the subsystems of the TSF are externally visible. ADV_HLD.1.7C

The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence. ADV_HLD.1.1E

The evaluator shall determine that the high-level design is an accurate and complete instantiation of the TOE security functional requirements. ADV_HLD.1.2E

5.2.3.3 Informal correspondence demonstration (ADV_RCR.1)

The developer shall provide an analysis of correspondence between all adjacent pairs of TSF representations that are provided. ADV_RCR.1.1D

For each adjacent pair of provided TSF representations, the analysis shall demonstrate that all relevant security functionality of the more abstract TSF representation is correctly and completely refined in the less abstract TSF representation. ADV_RCR.1.1C

The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence. ADV_RCR.1.1E

5.2.3.4 Informal TOE security policy model (ADV_SPM.1)

The developer shall provide a TSP model. ADV_SPM.1.1D

The developer shall demonstrate correspondence between the functional specification and the TSP model. ADV_SPM.1.2D

The TSP model shall be informal. ADV_SPM.1.1C

The TSP model shall describe the rules and characteristics of all policies of the TSP that can be modelled. ADV_SPM.1.2C

The TSP model shall include a rationale that demonstrates that it is consistent and complete with respect to all policies of the TSP that can be modelled. ADV_SPM.1.3C

The demonstration of correspondence between the TSP model and the functional specification shall show that all of the security functions in the functional specification are consistent and complete with respect to the TSP model. ADV_SPM.1.4C

The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence. ADV_SPM.1.1

5.2.4 Guidance Documents

5.2.4.1 Administrator guidance (AGD_ADM.1)

The developer shall provide administrator guidance addressed to system administrative personnel. AGD_ADM.1.1D

The administrator guidance shall describe the administrative functions and interfaces available to the administrator of the TOE. AGD_ADM.1.1C

The administrator guidance shall describe how to administer the TOE in a secure manner. AGD_ADM.1.2C

The administrator guidance shall contain warnings about functions and privileges that should be controlled in a secure processing environment. AGD_ADM.1.3C

The administrator guidance shall describe all assumptions regarding user behaviour that are relevant to secure operation of the TOE. AGD_ADM.1.4C

The administrator guidance shall describe all security parameters under the control of the administrator, indicating secure values as appropriate. AGD_ADM.1.5C

The administrator guidance shall describe each type of security-relevant event relative to the administrative functions that need to be performed, including changing the security characteristics of entities under the control of the TSF. AGD_ADM.1.6C

The administrator guidance shall be consistent with all other documentation supplied for evaluation. AGD_ADM.1.7C

The administrator guidance shall describe all security requirements for the IT environment that are relevant to the administrator. AGD_ADM.1.8C

The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence. AGD_ADM.1.1E

5.2.4.2 User guidance (AGD_USR.1)

The developer shall provide user guidance. AGD_USR.1.1D

The user guidance shall describe the functions and interfaces available to the non-administrative users of the TOE. AGD_USR.1.1C

The user guidance shall describe the use of user-accessible security functions provided by the TOE. AGD_USR.1.2C

The user guidance shall contain warnings about user-accessible functions and privileges that should be controlled in a secure processing environment. AGD_USR.1.3C

The user guidance shall clearly present all user responsibilities necessary for secure operation of the TOE, including those related to assumptions regarding user behaviour found in the statement of TOE security environment. AGD_USR.1.4C

The user guidance shall be consistent with all other documentation supplied for evaluation. AGD_USR.1.5C

The user guidance shall describe all security requirements for the IT environment that are relevant to the user. AGD_USR.1.6C

The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence. AGD_USR.1.1E

5.2.5 Tests

5.2.5.1 Evidence of coverage (ATE_COV.1)

The developer shall provide evidence of the test coverage. ATE_COV.1.1D

The evidence of the test coverage shall show the correspondence between the tests identified in the test documentation and the TSF as described in the functional specification. ATE_COV.1.1C

The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence. ATE_COV.1.1E

5.2.5.2 Functional testing (ATE_FUN.1)

The developer shall test the TSF and document the results. ATE_FUN.1.1D

The developer shall provide test documentation. ATE_FUN.1.2D

The test documentation shall consist of test plans, test procedure descriptions, expected test results and actual test results. ATE_FUN.1.1C

The test plans shall identify the security functions to be tested and describe the goal of the tests to be performed. ATE_FUN.1.2C

The test procedure descriptions shall identify the tests to be performed and describe the scenarios for testing each security function. These scenarios shall include any ordering dependencies on the results of other tests. ATE_FUN.1.3C

The expected test results shall show the anticipated outputs from a successful execution of the tests. ATE_FUN.1.4C

The test results from the developer execution of the tests shall demonstrate that each tested security function behaved as specified. ATE_FUN.1.5C

The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence. ATE_FUN.1.1E

5.2.5.3 Independent testing - sample (ATE_IND.2)

The developer shall provide the TOE for testing. ATE_IND.2.1D

The TOE shall be suitable for testing. ATE_IND.2.1C

The developer shall provide an equivalent set of resources to those that were used in the developer's functional testing of the TSF. ATE_IND.2.2C

The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence. ATE_IND.2.1E

The evaluator shall test a subset of the TSF as appropriate to confirm that the TOE operates as specified. ATE_IND.2.2E

The evaluator shall execute a sample of tests in the test documentation to verify the developer's test results. ATE_IND.2.3E

5.2.6 Vulnerability Assessment

5.2.6.1 Strength of TOE security function evaluation (AVA_SOF.1)

The developer shall perform a strength of TOE security function analysis for each mechanism identified in the ST as having a strength of TOE security function claim. AVA_SOF.1.1D

For each mechanism with a strength of TOE security function claim the strength of TOE security function analysis shall show that it meets or exceeds the minimum strength level defined in the PP/ST. AVA_SOF.1.1C

For each mechanism with a specific strength of TOE security function claim the strength of TOE security function analysis shall show that it meets or exceeds the specific strength of function metric defined in the PP/ ST. AVA_SOF.1.2C

The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence. AVA_SOF.1.1E

The evaluator shall confirm that the strength claims are correct. AVA_SOF.1.2

5.2.6.2 Developer vulnerability analysis (AVA_VLA.1)

The developer shall perform and document an analysis of the TOE deliverables searching for obvious ways in which a user can violate the TSP. AVA_VLA.1.1D

The developer shall document the disposition of obvious vulnerabilities. AVA_VLA.1.2D

The documentation shall show, for all identified vulnerabilities, that the vulnerability cannot be exploited in the intended environment for the TOE. AVA_VLA.1.1C

The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence. AVA_VLA.1.1E

The evaluator shall conduct penetration testing, building on the developer vulnerability analysis, to ensure obvious vulnerabilities have been addressed. AVA_VLA.1.2E

5.3 Security Requirements for the IT Environment

ITR.REVIEW$_{(CS)}$ Administrators will review audit records periodically, with the frequency of reviews to be determined by the responsible authorities of the enclave.

ITR.INSTALL$_{(SYS)}$ The TOE will be delivered and installed in a manner that maintains system security.

5.4 Security Requirements for the Non-IT Environment

NITR.PHYSICAL$_{(CS)}$ Appropriate physical controls will be used to protect the enclave.

NITR.TRAINING$_{(SYS)}$ Authorised users and administrators of the TOE will receive appropriate training in the secure operation of the TOE.

6—Rationale

6.1 Introduction and TOE Description Rationale

This section provides a set of rationale arguments for the PP.

Section 6.1 addresses threat and policy coverage by objectives and assumptions.

Section 6.2 addresses objective coverage by TOE and environmental components.

Section 6.3 addresses the adequacy of the assurance requirements (EAL2) chosen for this PP.

Section 6.4 addresses the minimum “strength of function” issues for this PP.

Section 6.5 addresses the dependency coverage for this PP.

Section 6.6 addresses the comprehensive argument that the PP’s IT requirements “form a mutually supportive and internally consistent whole.”

6.2 Security Objectives Rationale

This section contains a mapping table and individual arguments for each policy and threat that is covered. Table 6-1 lists either the organisational security policy or threat that requires coverage in the first column. Relevant and applicable assumptions are listed in the second column. Objectives that cover each policy and threat, given the applicable assumptions, are listed in the third column. Following this table are individual arguments for the coverage of each policy and threat.

Table 6-1. Tracing of Security Objectives to the TOE Security Environment

Policy/Threat	Assumptions	Objectives	
P.ACCOUNT	A.TRUSTED_ADMIN$_{(SYS)}$	O.AUDIT$_{(CS)}$ OE.REVIEW$_{(CS)}$	O.IDENTIFY$_{(SYS)}$
P.AUTHENTICATE	A.TRUSTED_USER$_{(RU)}$	O.MEDIA$_{(SYS)}$ OE.TRAIN$_{(SYS)}$	OE.PHYSICAL$_{(SYS)}$
P.BANNER		O.BANNER$_{(SYS)}$	
P.CONFIDENTIALITY	A.TRUSTED_ADMIN$_{(SYS)}$ A.TRUSTED_USER$_{(RU)}$	O.MEDIA$_{(RU)}$ O.IDENTIFY$_{(SYS)}$ O.RECEIVE$_{(SYS)}$	O.ACCESS$_{(SYS)}$ O.NO_EAVESDROP$_{(SYS)}$ O.ACCESS$_{(RU)}$
P.ELGIBLE		O.ACCESS$_{(SYS)}$ O.MEDIA$_{(RU)}$	OE.PHYSICAL$_{(SYS)}$ O.ACCESS$_{(RU)}$

Policy/Threat	Assumptions	Objectives
P.EXPORT	A.TRUSTED_USER$_{\text{(RU)}}$ A.TRUSTED_ADMIN$_{\text{(SYS)}}$	O.MEDIA$_{\text{(RU)}}$ OE.TRAIN$_{\text{(SYS)}}$
P.INTEGRITY	A.TRUSTED_USER$_{\text{(RU)}}$ A.TRUSTED_ADMIN$_{\text{(SYS)}}$	O.DETECT$_{\text{(RU)}}$ O.ACCESS$_{\text{(SYS)}}$ O.ACCESS$_{\text{(RU)}}$ O.IDENTIFY$_{\text{(SYS)}}$ O.RECEIVE$_{\text{(SYS)}}$ O.ANTIVIRUS$_{\text{(SYS)}}$
P.MANAGE	A.TRUSTED_ADMIN$_{\text{(SYS)}}$	O.MANAGE$_{\text{(SYS)}}$ OE.INSTALL$_{\text{(SYS)}}$ OE.TRAIN$_{\text{(SYS)}}$
P.PROCEDURES	A.TRUSTED_USER$_{\text{(RU)}}$ A.TRUSTED_ADMIN$_{\text{(SYS)}}$	O.MANAGE$_{\text{(SYS)}}$ OE.TRAIN$_{\text{(SYS)}}$
P.REMOTE_ADMIN	A.TRUSTED_ADMIN$_{\text{(SYS)}}$	O.ACCESS$_{\text{(RU)}}$ O.CRYPTO_SUPPORT$_{\text{(SYS)}}$ O.IDENTIFY$_{\text{(SYS)}}$
P.TRAINING	A.TRUSTED_USER$_{\text{(RU)}}$ A.TRUSTED_ADMIN$_{\text{(SYS)}}$	OE.TRAIN$_{\text{(SYS)}}$
T.ALTER	A.TRUSTED_USER$_{\text{(RU)}}$ A.TRUSTED_ADMIN$_{\text{(SYS)}}$	O.DETECT$_{\text{(RU)}}$ OE.PHYSICAL$_{\text{(SYS)}}$ O.ANTIVIRUS$_{\text{(SYS)}}$ O.ACCESS$_{\text{(RU)}}$ O.ACCESS$_{\text{(SYS)}}$ O.AUDIT$_{\text{(CS)}}$
T.AUD_FAIL		O.AUDIT$_{\text{(CS)}}$ O.SELF_PROTECT$_{\text{(SYS)}}$ OE.TRAIN$_{\text{(SYS)}}$
T.AUD_REV	A.TRUSTED_ADMIN$_{\text{(SYS)}}$	OE.REVIEW$_{\text{(CS)}}$ OE.TRAIN$_{\text{(SYS)}}$
T.BACKUP		OE.BACKUP$_{\text{(CS)}}$ OE.TRAIN$_{\text{(SYS)}}$
T.CAPTURE	A.AVAILABLE$_{\text{(SYS)}}$	O.NO_EAVESDROP$_{\text{(SYS)}}$ O.RECEIVE$_{\text{(SYS)}}$ O.SELF-PROTECT$_{\text{(SYS)}}$ OE.PHYSICAL$_{\text{(SYS)}}$
T.CRYPTANALYTIC	A.CRYPTANALYTIC	O.ACCESS$_{\text{(SYS)}}$ O.SELF_PROTECT$_{\text{(SYS)}}$
T.DENIAL	A.LIM_ACCESS$_{\text{(CS)}}$	O.ANTIVIRUS$_{\text{(SYS)}}$ O.AUDIT$_{\text{(CS)}}$ O.IDENIFY$_{\text{(SYS)}}$ O.SELF_PROTECT$_{\text{(SYS)}}$ OE.REVIEW$_{\text{(CS)}}$ O.CS_AVAILABLE$_{\text{(CS)}}$
T.ERROR	A.TRUSTED_USER$_{\text{(RU)}}$ A.TRUSTED_ADMIN$_{\text{(SYS)}}$	O.DETECT$_{\text{(RU)}}$ O.RECEIVE$_{\text{(SYS)}}$ O.SELF_PROTECT$_{\text{(SYS)}}$
T.IMPORT	A.TRUSTED_USER$_{\text{(RU)}}$ A.TRUSTED_ADMIN$_{\text{(SYS)}}$	O.ANTIVIRUS$_{\text{(SYS)}}$
T.INTRUDE	A.TRUSTED_ADMIN$_{\text{(SYS)}}$ A.LIM_ACCESS$_{\text{(CS)}}$	O.DETECT$_{\text{(RU)}}$ O.ACCESS$_{\text{(SYS)}}$ O.IDENTIFY$_{\text{(SYS)}}$ OE.PHYSICAL$_{\text{(SYS)}}$
T.MASQUERADE		O.IDENTIFY$_{\text{(SYS)}}$

Policy/Threat	Assumptions	Objectives
T.MEDIA	A.LIM_ACCESS$_{(CS)}$	OE.BACKUP$_{(CS)}$ OE.INSTALL$_{(SYS)}$ OE.TRAIN$_{(SYS)}$ OE.PHYSICAL$_{(SYS)}$ O.MEDIA$_{(RU)}$
T.MODIFY	A.LIM_ACCESS$_{(CS)}$ A.TRUSTED_ADMIN$_{(SYS)}$	O.ACCESS$_{(SYS)}$ O.AUDIT$_{(CS)}$ O.SELF_PROTECT$_{(SYS)}$ OE.REVIEW$_{(CS)}$
T.PHYSICAL	A.LIM_ACCESS$_{(CS)}$	O.DETECT$_{(RU)}$ OE.PHYSICAL$_{(SYS)}$
T.REPEAT	A.TRUSTED_ADMIN$_{(SYS)}$	O.AUDIT$_{(CS)}$ O.IDENTIFY$_{(SYS)}$ OE.REVIEW$_{(CS)}$ O.SELF_PROTECT$_{(SYS)}$
T.REPUDIATION	A.TRUSTED_USER$_{(RU)}$ A.TRUSTED_ADMIN$_{(SYS)}$	O.AUDIT$_{(CS)}$ O.CRYPTO_SUPPORT$_{(SYS)}$ O.IDENTIFY$_{(SYS)}$
T.TRAFFIC	A.AVAILABLE$_{(SYS)}$	O.RECEIVE$_{(SYS)}$ OE.TRAIN$_{(SYS)}$ O.SELF-PROTECT$_{(SYS)}$ O.NO_EAVESDROP$_{(SYS)}$
T.UNDETECT	A.TRUSTED_USER$_{(RU)}$ A.TRUSTED_ADMIN$_{(SYS)}$	O.DETECT$_{(RU)}$ O.AUDIT$_{(CS)}$ O.MANAGE$_{(SYS)}$ OE.REVIEW$_{(CS)}$ OE.TRAIN$_{(SYS)}$

6.2.1 Policies

P.ACCOUNT User activity shall be monitored to the extent that sanctions can be applied when malfeasance occurs, and to ensure that system controls are properly applied.

Users are required to be identified and authenticated by the O.IDENTIFY$_{(SYS)}$ objective. Once access to the TOE has been established, the O.AUDIT$_{(CS)}$ objective requires an audit trail to be kept for user activity, and to allow association of user actions with identified individuals. Finally, the OE.REVIEW$_{(CS)}$ objective requires administrators to perform reviews periodically, so that the audit trails are actually used to review user activity. A.TRUSTED_ADMIN$_{(SYS)}$ assumes that administrators are competent to determine malfeasance from observation of audit logs on the system, and that they take appropriate actions when malfeasance is detected. This also assumes that system functions supporting these objectives will be competently managed.

P.AUTHENICATE The TOE will require users to be authenticated to the system before access to system resources is allowed.

The user of the TOE is assumed to be trusted (A.TRUSTED_USER$_{(RU)}$) but will require authentication to the remote access unit before access to system resources is allowed. The system resources are protected from unauthorised access when the system is powered off (O.MEDIA$_{(SYS)}$) and will only allow access to authorised users(OE.PHYSICAL$_{(SYS)}$). Users are trained (OE.TRAIN$_{(SYS)}$) to operate the system and to use proper authentication.

P.BANNER The TOE will provide a banner to notify administrators that they have entered a Government computer system.

This policy intends to notify administrators that they have entered a Government computer system before establishing an administrator session (O.BANNER$_{(SYS)}$).

P.CONFIDENTIALITY The TOE shall provide controls that are adequate to protect the confidentiality of user data and TSF data.

All individuals using the system are uniquely identified and authenticated (O.IDENTIFY$_{(SYS)}$), thus allowing accountability for access to data. For data subject to the enclave security policy, that policy as defined for the accountable individual, including disclosure, is enforced (O.ACCESS$_{(SYS)}$). For data being transferred using the TN, the TOE prevents disclosure to eavesdroppers with a strength appropriate to the data (O.NO_EAVESDROP$_{(SYS)}$). The only channels to the data on an RU are to the authenticated user, who does not intentionally violate organisational security policies (A.TRUSTED_USER$_{(RU)}$), and through the TN to a mutually authenticated CS (O.RECEIVE$_{(SYS)}$); when the TOE is not operating, protected data is inaccessible (O.MEDIA$_{(RU)}$). Likewise, the CS is only accessible through the TN to a mutually authenticated MU (O.RECEIVE$_{(SYS)}$), through the enclave. The remote user must authenticate to the remote system before access to system resources is allowed (O.ACCESS$_{(RU)}$) including communications channels used to establish a connection to the TN. Administrators are trusted not to abuse their privileges (A.TRUSTED_ADMIN$_{(SYS)}$); thus no unauthorised users will be provided access to the system.

P.ELGIBLE Authorised users and administrators of the TOE shall be eligible to access information that is created, communicated, processed, or stored on the TOE.

This policy focuses on the eligibility of users to access the TOE. The policy is met by ensuring that all users (and administrators) of the TOE have an appropriate need to know for the information handled by the TOE.

Only authorised users and administrators of the protected enclave are eligible to access information that is created, communicated, processed, or stored within the enclave. Users and administrators must be granted access to system resources contained on the TOE (O.ACCESS $_{(RU)}$ and O.ACCESS$_{(SYS)}$), requiring that all users and administrators of the TOE have an appropriate clearance level for the information handled by the TOE. All physical protection of the TOE hardware, software, documentation, and sensitive data is established by (OE.PHYSICAL$_{(SYS)}$). The protection of data stored on the RU while it is not in use is provided by O.MEDIA$_{(RU)}$.

P.EXPORT Authorised users and administrators of the TOE shall not export information processed by the TOE without proper and explicit authorisation.

The control of information export cannot be based entirely upon a function of technological controls for multi-user information systems, but must always rely on policy-conformant behaviour by the users.

While the RU is not in use, its information is not available to unauthorised users through O.MEDIA$_{(RU)}$. Information cannot be exported from the RU without explicit actions by the remote user. User information is protected outside of the enclave (during storage on the RU, transit, and connection establishment).

Users and administrators of the system are assumed to be competent and compliant to organisational security policies (A.TRUSTED_USER$_{(RU)}$ and A.TRUSTED_ADMIN$_{(SYS)}$). Finally, users and administrators of the system will be trained for appropriate procedures that prevent unauthorised and/or unwitting export of SBU information from the TOE (OE.TRAIN$_{(SYS)}$).

P.INTEGRITY The TOE shall provide controls that are adequate to protect the integrity of user data.

All individuals using the system are uniquely identified and authenticated (O.IDENTIFY$_{(SYS)}$), thus allowing accountability for access to data. Access to TOE resources including user data is protected from unauthorised access by the objectives (O.ACCESS$_{(RU)}$) and (O.ACCESS$_{(SYS)}$). Data being transferred using the TN, the TOE detects and discards any data that does not originate from another CS or RU that is mutually authenticated (O.RECEIVE$_{(SYS)}$). The only channels to the data on an RU are to the authenticated user, who does not intentionally violate organisational security policies (A.TRUSTED_USER$_{(RU)}$), and through the TN to a mutually authenticated CS (O.RECEIVE$_{(SYS)}$). When the TOE is not operating, modifications to protected data are detected (O.DETECT$_{(RU)}$). Likewise, the CS is only accessible through the TN to a mutually authenticated RU (O.RECEIVE$_{(SYS)}$), through the enclave, and with administrators who are trusted not to abuse their privileges (A.TRUSTED_ADMIN$_{(SYS)}$). Malicious code detection and removal is accomplished through the use of antivirus software to protect system resources and user data (O.ANTIVIRUS$_{(SYS)}$).

P.MANAGE The TOE shall be managed such that its security functions are implemented and preserved throughout its operational lifetime.

This policy is covered by requiring management support via O.MANAGE$_{(SYS),}$ as well as trained and competent administrators (A.TRUSTED_ADMIN$_{(SYS)}$) who are adequately trained (OE.TRAIN$_{(SYS)}$) to manage the system in its operational environment.

O.MANAGE$_{(SYS)}$ is a comprehensive objective, and the actual functionality required depends heavily upon the security functions provided by the TOE. O.MANAGE$_{(SYS)}$ applies to the TOE as a whole, as the management of security functions should be uniformly adequate, regardless of partition environment. Security attributes must be managed and assigned secure values, and the TOE must be configurable by administrators to support the system's security policies. Security functions that implement protection on the system must be managed by administrators. Administrators should be able to revoke access to the TOE, so that the TOE's policy enforcement can accurately reflect real-world changes in user authorisations. Management of the TOE depends on proper installation of security enforcement and security management functions (OE.INSTALL$_{(SYS)}$).

P.PROCEDURES Procedures will be in place to restrict inadvertent disclosures or modification of sensitive information or improper utilisation of resources in the TSE.

The assumptions A.TRUSTED_USER$_{(RU)}$, and TRUSTED_ADMIN$_{(SYS)}$ support this policy by assuming the users and administrators will not intentionally disclose or modify sensitive information, and they will take the necessary precautions to prevent against such activities happening. O.MANAGE$_{(SYS)}$ provides the administrator with adequate management features for all security functions. OE.TRAIN$_{(SYS)}$ will ensure that administrators are trained on these management features so as to provide support for P.PROCEDURES.

P.REMOTE_ADMIN Authorised administrators may remotely administer devices in the TSE through protected external communication channels.

Remote administration of protected equipment often presents additional security challenges. In order to allow remote administration and prevent violations of the TSP during a remote administration session, the administrator must be trusted (A.TRUSTED_ADMIN$_{(SYS)}$). Access control mechanisms at the remote workstation must also be in place provide the necessary access control and I&A mechanisms to the administrator (O.ACCESS$_{(RU)}$, O.IDENTIFY$_{(SYS)}$). O.CRYPTO_SUPPORT$_{(SYS)}$ also supports this policy by preventing any disclosure of information transmitted across the TN during a remote administration session.

P.TRAINING All TOE users and administrators shall be properly trained on the TSF prior to accessing an operational TOE.

Users and administrators are trained and aware of unique system responsibilities for their individual roles(OE.TRAIN$_{(SYS)}$). The assumption that trained users and administrators are trusted is important to the expectation of proper implementation of training and policy (A.TRUSTED_USER$_{(RU)}$ and A.TRUSTED_ADMIM$_{(SYS)}$).

6.2.2 Threats

T.ALTER An unauthorised user may surreptitiously gain access to the TOE and attempt to alter and/or replace system elements (e.g., hardware, firmware, or software) in an attempt to subvert the device.

There will be environmental support for the TOE (OE.PHYSICAL$_{(SYS)}$) to provide protection against physical alterations of the system. This support is augmented by O.DETECT$_{(RU)}$ and A.TRUSTED_USER$_{(RU)}$ which places the RU under the control of a trusted user and provides a mechanism to detect unauthorised changes to it's configuration. A.TRUSTED_ADMIN$_{(SYS)}$ assumes that competent system administrators will be observant of the CS in the enclave environment and therefore will be cognisant of unauthorised physical alterations.

O.ACCESS$_{(SYS)}$ and O.ACCESS$_{(RU)}$ limit access to both the communications server and the remote unit such that only authorised individuals may access the system elements. Furthermore, O.AUDIT$_{(CS)}$ will provide a record of any attempted system modifications. Should any malicious software be added or modified within the TOE, O.ANTIVIRUS$_{(SYS)}$ provides malicious code detection and elimination capabilities for the TOE.

T.AUD_FAIL System modification, compromise, or audit file full may result in failure to collect audit data.

Protection against failed audit data collection is provided primarily by the TOE system itself. Administrators must also be properly trained on the audit system (OE.TRAIN$_{(SYS)}$). Use of the audit function will ensure all necessary audit data is collected (O.AUDIT$_{(CS)}$). Furthermore, the system should protect against any attempt to modify audit data (O.SELF_PROTECT$_{(SYS)}$) which may compromise TOE security.

T.AUD_REV Appropriate individuals may fail to adequately review and interpret the audit data, or take appropriate action.

System security functions, such as audit, require the periodic review (OE.REVIEW$_{(CS)}$) and analysis of audit data to detect suspicious activity. It is assumed the administrators are non-hostile and competent but may fail in certain aspects of their duties (A.TRUSTED_ADMIN$_{(SYS)}$). Training (OE.TRAIN$_{(SYS)}$) for administrators should emphasise audit data review and establish required actions when suspicious activity is detected.

T.BACKUP Failure to adequately perform system backup may result in compromise or system non-availability.

The TOE enables communications into a secure enclave for remote users. Resources requiring backup reside on both the RU and the CS portions of the TOE. The system resources will be protected from destruction by periodic backups (OE.BACKUP$_{(CS)}$). Users and administrators will be trained (OE.TRAIN$_{(SYS)}$) on system backup and restore procedures for the TOE. Failure to perform backups or to properly restore the system, especially the CS element, may result in lengthy downtime or system outage.

T.CAPTURE An agent may eavesdrop on, or otherwise capture, data being transferred on a communications channel.

The communications channel is assumed to be available during operation of the TOE (A.AVAILABLE$_{(SYS)}$). Although this assumption resolves an availability concern, it introduces a property that threat agents within the TN will always be present within the system. Subsequently, O.NO_EAVESDROP$_{(SYS)}$ protects the confidentiality of data within the TN with mechanisms that are appropriate for SBU-level information. O.RECEIVE$_{(SYS)}$ protects against unauthorised connections between CS and RU partitions, preventing spoofing attacks that might be initiated by a malicious host on the TN that is intercepting connection set-up traffic. The combination of OE.PHYSICAL$_{(SYS)}$ and O.SELF-PROTECT$_{(SYS)}$ protect against physical and penetration attacks (respectively) that undermine the implementation of O.NO_EAVESDROP$_{(SYS)}$, which provides the protection of the communications channel.

T.CRYPTANALYTIC Unauthorised agents may passively attack the cryptography of the TOE using cryptanalysis methods.

A.CRYPTANALYTIC assumes the cryptographic methods are sufficiently strong to protect sensitive data from passive cryptanalytic attacks. O.ACCESS$_{(SYS)}$ controls access to the cryptographic elements of the TOE based on the identity of the accountable individual. Thus, an unauthorized agent cannot bypass the access control policy in the TOE. Also, O.SELF_PROTECT$_{(SYS)}$ ensures the TOE cryptographic functions are protected against external interference or tampering.

T.DENIAL An unauthorised user may render the TOE unavailable for use.

Protection against a denial of service attack can be broken down into physical and logical protections. By limiting access to authorised individuals, A.LIM_ACCESS$_{(CS)}$ assumes the CS is somewhat protected against physical attacks that may render the TOE inoperable. Both physical and logical protection of the TOE is provided by O.SELF_PROTECT$_{(SYS)}$, which ensures TOE security functions operate properly and cannot be bypassed by unauthorised users. O.CS_AVAILABLE$_{(CS)}$ prevents a single user identity from connecting to more than one CS modem at a time, thus preventing the possibility of a denial of service by simultaneously connecting to all available modems. Although total protection against a denial of service attack is unrealistic, some degree of protection for TOE software functionality against malicious code is provided by O.ANTIVIRUS$_{(SYS)}$. Furthermore, unique identification of all users and administrators (O.IDENTIFY$_{(SYS)}$), as well as continuous monitoring of all system activities (O.AUDIT$_{(CS)}$, OE.REVIEW$_{(CS)}$) provides for non-repudiation. Denial of service attacks against the CS interface to the TN such as war dialling cannot reasonably be addressed by the TSF.

T.ERROR A user may attempt to perform unauthorised or erroneous actions that will compromise user and/or system resources.

The threat of a user performing unauthorised or erroneous actions that will compromise user and/or system resources (O.SELF_PROTECT$_{(SYS)}$); is addressed at the RU by O.DETECT$_{(RU)}$ which ensures that the RU will detect unauthorised changes to its configuration. O.RECEIVE$_{(SYS)}$ which ensures that an RU will only communicate with a CS with which it has mutually authenticated. The assumption A.TRUSTED_USER$_{(RU)}$ states that the users will not intentionally violate organisational security policies. A.TRUSTED_ADMIN$_{(SYS)}$, assumes that the administrators will not deliberately abuse their privileges so as to violate security policies.

T.IMPORT An authorised user or administrator of the TOE may unwittingly introduce malicious code into the system, resulting in a compromise of the integrity and/or availability of system resources.

O.ANTIVIRUS$_{(SYS)}$ will provide effective malicious code detection and elimination, should such code be loaded into the system. A.TRUSTED_USER$_{(RU)}$ assumes that the users will not intentionally violate organisational security policies. A.TRUSTED_ADMIN$_{(SYS)}$, assumes that the administrators will not deliberately abuse their privileges so as to violate security policies.

T.INTRUDE An unauthorised user may use the TOE to gain access to the secure enclave.

The TOE provides an interface to the secure enclave that may be outside the normal physical and procedural controls of the organisation. With the exception of the CS interface to the TN, the CS is located within the domain of physical control of the secure enclave and has limited authorised access to it (A.LIM_ACCESS$_{(CS)}$).

It is assumed that the strength of the authentication mechanisms that are used for the TOE are suitable for access to the enclave through the CS interface to the enclave boundary. O.ACCESS$_{(SYS)}$ ensures that an authenticated user only accesses information that would have been allowed within the protected enclave. OE.PHYSICAL$_{(SYS)}$ provides protection from unauthorised access from TOE resources and SBU data.

O.IDENTIFY $_{(SYS)}$ ensures that an active connection of an RU to a CS requires that a valid user was properly identified and authenticated. Meeting the objective O.DETECT$_{(RU)}$ protects against an intruder indirectly gaining access to the enclave through the RU. A.TRUSTED_ADMIN$_{(SYS)}$ states that the administrators will not deliberately abuse their privileges so as to violate security policies.

T.MASQUERADE An unauthorised user may attempt to gain access to the TOE by pretending to be an authorised user.

A threat agent may impersonate an authorised user or administrator of the system and this is addressed by the security objective O.IDENTIFY$_{(SYS)}$, which provides for authentication of users.

T.MEDIA Failure to adequately protect storage media may result in compromise or non-availability of the TOE.

Access to storage media for the CS is minimised by the assumption A.LIM_ACCESS$_{(CS)}$. While the remote unit is powered off O.MEDIA$_{(RU)}$ will protect the stored data. Proper delivery, installation, handling, management, operation, and backup of the TOE (OE.INSTALL$_{(SYS)}$, OE.BACKUP$_{(CS)}$,OE_PHYSICAL$_{(SYS)}$) and the associated training for the individuals supporting these activities (OE.TRAIN$_{(SYS)}$) also reduces the threat to the TOE media.

T.MODIFY An unauthorised modification of the audit data may occur.

There will be environmental support of the TOE to provide protection against audit data modifications provided by A.LIM_ACCESS$_{(CS).}$ TOE users are restricted to information that is allowed to them within the secure network (O.ACCESS$_{(SYS)}$), meaning that users do not have access to the audit data. O.AUDIT$_{(CS)}$ provides for audit of user and administrator actions. An operational audit system will provide protection against tampering or bypassing security functions (O.SELF_PROTECT$_{(SYS)}$). A.TRUSTED_ADMIN$_{(SYS)}$ will not intentionally modify data. The administrators will review audit data to identify unauthorised activity(OE.REVIEW$_{(CS)}$).

T.PHYSICAL

TOE security functions (TSF) may be subject to physical attack that may compromise security.

Physical threats on the RU can be mitigated by OE.PHYSICAL$_{\text{(SYS)}}$. Detecting when an attack modifies the RU configuration (O.DETECT$_{\text{(RU)}}$). Within the CS environment, additional controls are necessary. A.LIM_ACCESS$_{\text{(CS)}}$ assumes that the CS partition is isolated from non-administrative users within the enclave. In particular, this implies that users that are authorised to be within the enclave but not authorised to access the TOE are physically isolated from the TOE.

T.REPEAT

An unauthorised user may repeatedly attempt to guess authentication information.

Access to TOE resources will require each user to be uniquely identified(O.IDENTIFY$_{\text{(SYS)}}$). All connection attempts are logged into audit data (O.AUDIT$_{\text{(CS)}}$) that is reviewed (OE.REVIEW$_{\text{(CS)}}$) to identify repeated attempts to guess authentication. The TOE will be protected from users attempting to bypass, interfere, or tamper with its security functions (O.SELF_PROTECT$_{\text{(SYS)}}$). A.TRUSTED_ADMIN$_{\text{(SYS)}}$ assumes that all administrators are well trained, non-hostile and follow proper security procedures.

T.REPUDIATION

Authorised users or administrators may deny originating or receiving data transfers or performing malicious acts.

A.TRUSTED_USER$_{\text{(RU)}}$ and A.TRUSTED_ADMIN$_{\text{(SYS)}}$ assume that the user and the administrator are trusted to not maliciously modify or delete the audit records at the RU and CS site, respectively. The audit records (O.AUDIT$_{\text{(CS)}}$) as well as O.CRYPTO_SUPPORT$_{\text{(SYS)}}$ provide protection against an entity claiming to have not participated in a communication. O.IDENTIFY$_{\text{(SYS)}}$ provides a mechanism to uniquely identify and authenticate individuals. Thus, based on the integrity of files and configuration parameters, and an un-modifiable audit log, an entry in the audit log that corresponds to a particular user can be used as proof of that user’s participation in a particular communication.

T.TRAFFIC

Use of the TOE may transmit (via traffic analysis or covert channel analysis) sensitive information to unauthorised users. (Port emanations)

The TOE must establish communications via the TN (A.AVAILABLE$_{\text{(SYS)}}$). O.RECEIVE$_{\text{(SYS)}}$ will ensure that the connection made between the RU and the CS is allowed and O.NO_EAVESDROP$_{\text{(SYS)}}$ will ensure that there is no disclosure of information. OE.TRAIN$_{\text{(SYS)}}$ and O.SELF_PROTECT$_{\text{(SYS)}}$ will ensure that the user will know if they have established a secure link or not.

T.UNDETECT

Compromises of user resources or system resources (by any threat agent) may go undetected for long periods of time.

The basic mechanism that is used by the TOE to counter this threat is O.AUDIT$_{(CS)}$. This objective provides for an audit trail by which the actions of both users and administrators are recorded by the system, and subsequently held accountable for their actions. OE.REVIEW$_{(CS)}$ ensures that the audit trail will be reviewed by administrators who will be able to reconstruct events and to determine the magnitude of compromises, if they should occur. O.DETECT$_{(RU)}$ allows unauthorised changes to the RU configuration to be made known immediately. Because of A.TRUSTED_USER$_{(RU)}$, there is assurance that the remote user will report these unauthorised changes to administrative personnel.

O.MANAGE$_{(SYS)}$ allows for management of audit mechanisms and any review functions. OE.TRAIN$_{(SYS)}$ seeks to ensure that administrators are able to perform effective maintenance and review of the audit trail. Typically, such training (along with A.TRUSTED_ADMIN$_{(SYS)}$) will result in administrators that can identify security-relevant events and react appropriately.

6.3 Security Requirements Rationale

6.3.1 Functional Security Requirements Rationale

This section contains a mapping table and individual arguments for each objective covered.

This section is contains a mapping table and individual arguments for each objective covered. Table 6-2 lists either the TOE or environmental Objective that requires coverage in the first column. The second column provides a cross index of Policies and/or Threats that are addressed, in part or in full, but each Objective. TOE components and/or environmental requirements that cover each Objective are listed in the third column. Following this table are individual arguments for the coverage of each Objective.

Table 6-2. Functional Component to Security Objective Mapping

Objectives	Requirements		
O.ACCESS$_{(RU)}$	FDP_ACC.1$_{(RU)}$	FDP_ACF.1	FIA_UAU.2
	FIA_UAU.6	FTA_SSL.1$_{(RU)}$	
O.ACCESS$_{(SYS)}$	FDP_IFC.1$_{(CS)}$	FDP_IFF.1$_{(CS)}$	FDP_IFC.1$_{(SYS)}$
	FDP_IFF.1$_{(SYS)}$	FDP_ITT.1$_{(SYS)}$	FDP_ITT.3$_{(SYS)}$
	FDP_RIP.2$_{(RU)}$	FCO_NRO.2$_{(SYS)}$	FTA_SSL.1$_{(CS)}$
O.ANTIVIRUS$_{(SYS)}$	FDP_SDI.2		
O.AUDIT$_{(CS)}$	FIA_UID.2$_{(SYS)}$	FIA_UAU.2$_{(SYS)}$	FIA_USB.1$_{(CS)}$
	FAU_GEN.1$_{(CS)}$	FAU_GEN.2$_{(CS)}$	FAU_ARP.1$_{(CS)}$
	FAU_SAA.1$_{(CS)}$	FAU_SAR.1$_{(CS)}$	FAU_SAR.2$_{(CS)}$

Objectives	Requirements		
	FAU_SAR.3$_{(CS)}$	FAU_STG.1$_{(CS)}$	FAU_STG.4$_{(CS)}$
	FPT_STM.1$_{(CS)}$	FCO_NRO.2$_{(SYS)}$	
O.BANNER$_{(SYS)}$	FTA_TAB.1$_{(SYS)}$		
O.CRYPTO_SUPPORT$_{(SYS)}$	FMT_MTD.1$_{(SYS)}$	FIA_ATD.1$_{(SYS)}$	FIA_SOS.1$_{(SYS)}$
	FPT_STM$_{(CS)}$		
O.CS_AVAILABLE$_{(CS)}$	FRU_RSA.1$_{(CS)}$		
O.DETECT$_{(CS)}$	FAU_ARP.1$_{(SYS)}$	FAU_SAA.3$_{(CS)}$	
O.IDENTIFY$_{(SYS)}$	FIA_UAU.6	FIA_UAU.2$_{(SYS)}$	FIA_AFL1$_{(CS)}$
	FIA_UID.2$_{(SYS)}$	FIA_UAU.7$_{(SYS)}$	FIA_AFL.1$_{(RU)}$
	FCO_NRO.2$_{(SYS)}$		
O.INTEGRITY$_{(SYS)}$	FCS_COP.1	FIA_SOS.2	FPT_STM.1
O.MANAGE$_{(SYS)}$	FMT_MOF.1$_{(SYS)}$	FMT_MSA.3$_{(SYS)}$	FMT_SMR.1$_{(SYS)}$
	FMT_MOF.1$_{(RU)}$	FMT_MTD.1$_{(SYS)}$	FAU_SAR.1
	FMT_MSA.1$_{(SYS)}$	FMT_REV.1$_{(SYS)}$	FAU_SAR.2
	FMT_MSA.2$_{(SYS)}$	FMT_SAE.1$_{(CS)}$	FAU_SAR.3
O.MEDIA$_{(RU)}$	FCS_COP.1$_{(RU)}$	FDP_RIP.2$_{(RU)}$	FTA_SSL.1$_{(RU)}$
O.NO_EAVESDROP$_{(SYS)}$	FCS_CKM.1	FCS_CKM.4	FCS_COP.1$_{(CS)}$
	FCS_CKM.2	FCS_COP.1$_{(CS)}$	FDP_ITT.1$_{(SYS)}$
O.RECEIVE$_{(SYS)}$	FDP_IFF.1$_{(CS)}$	FDP_IFC.1$_{(SYS)}$	FCS_COP.1$_{(CS)}$
	FDP_IFF.1$_{(SYS)}$	FDP_IFC.1$_{(CS)}$	FCS_COP.1$_{(RU)}$
	FCO_NRO.2$_{(SYS)}$		
O.SECURE_STARTUP$_{(SYS)}$	FPT_RCV.2$_{(SYS)}$		
O.SELF_PROTECT$_{(SYS)}$	FPT_ITT.2$_{(SYS)}$	FPT_RPL.1$_{(SYS)}$	FPT_SEP.1$_{(SYS)}$
	FPT_ITT.3$_{(SYS)}$	FPT_RVM.1$_{(SYS)}$	
O.SELF_TEST$_{(SYS)}$	FIA_SOS.1$_{(SYS)}$	FPT_AMT.1$_{(SYS)}$	FPT_TST.1$_{(SYS)}$
	FIA_SOS.2$_{(SYS)}$		
OE.BACKUP$_{(CS)}$	FAU_STG.2$_{(CS)}$	FAU_STG.4$_{(CS)}$	FMT_MTD.1$_{(SYS)}$
OE.INSTALL$_{(SYS)}$	FMT_MOF.1	FMT_MSA.3$_{(SYS)}$	ITR.INSTALL$_{(SYS)}$
OE.PHYSICAL$_{(SYS)}$	NITR_PHYSICAL$_{(CS)}$		
OE.REVIEW$_{(CS)}$	FAU_SAR.1	FAU_SAR.3	ITR_REVIEW$_{(CS)}$
	FAU_SAR.2		
OE.TRAIN$_{(SYS)}$	NITR.TRAINING$_{(SYS)}$		

O.ACCESS$_{\text{(SYS)}}$ The TOE will control access to information that is subject to the enclave security policy, based on the identity of the accountable individuals, such that this policy cannot be bypassed in the TOE.

Users can access data controlled by the TOE either through the enclave or through a remote unit. The enclave will only deliver data to an enclave session on the CS if its security policy allows reading by the accountable individual for that session. The CS will only allow this data to flow to the RU connection associated with that session (FDP_IFC.1$_{\text{(CS)}}$ and FDP_IFF.1$_{\text{(CS)}}$). The data sent by the CS across the TN will only be readable by the corresponding RU, being used by the same accountable individual as is associated with the enclave session. Since the user of the RU was authorised to read the data, the RU only must protect that data when the user is not present (FDP_RIP.2$_{\text{(RU)}}$). Data and commands sent from a RU to the CS are identified with the user of the RU. They cannot be modified while in the TN (FDP_ITT.1$_{\text{(SYS)}}$). They will be kept separate from all other information received by the CS from remote sources (FDP_IFC.1$_{\text{(SYS)}}$, FDP_IFF.1$_{\text{(SYS)}}$). The CS will only allow this information to flow to the enclave session associated with the remote connection (FDP_IFC.1$_{\text{(CS)}}$ and FDP_IFF.1$_{\text{(CS)}}$). The enclave will treat these commands and data according to its security policy. This objective also supports the non-repudiation of origin requirements (FCO_NRO.2$_{\text{(SYS)}}$) by controlling access based on the identified individual. For all transmissions the individual can thus be held accountable.

If an administrator is running an administrator session on the CS, and steps away from the terminal for a period of time, the session locking requirement (FTA_SSL.1$_{\text{(CS)}}$) will prevent an unauthorized user from using the terminal.

O.ACCESS$_{\text{(RU)}}$ During operation the RU would limit access to system resources to authorised users.

FDP_ACC.1 and FDP_ACF.1 enforce access control policies (P.RU_ACCESS and P.USER_ACCESS) at the RU. Users of the RU are required to be authenticated before performing any actions on the RU (FIA_UAU.2(SYS)). If an authorized user is connected in a remote session to the CS, and steps away from the terminal for a period of time, the session locking requirement (FTA_SSL.1$_{\text{(RU)}}$) will prevent an unauthorized user from using the terminal. Additionally, when session locking is triggered users must re-authenticate to the RU (FIA_UAU.6(RU)).

O.ANTIVIRUS$_{\text{(SYS)}}$ The TOE will provide for effective malicious code detections and elimination.

The requirement FDP_SDI.2 meets this objective by monitoring TSF data for malicious code and other data integrity errors. If error are detected, and administrator is alerted, and the errors will be eliminated by the administrator.

O.AUDIT$_{(CS)}$

The TOE will provide an audit trail to ensure each authenticated user and TOE administrator can be held accountable for his or her actions in the TOE. The audit trail will be of sufficient detail to reconstruct events in determining the cause or magnitude of compromise should a security violation or malfunction occur.

Several requirements are included here to address the O.AUDIT objective, which essentially provides the non-repudiation function for the TOE. The requirement FAU_GEN.1 calls for an audit function in the TOE. Additionally, FAU_GEN.1 specifically lists which events are auditable during operation of the TOE. Attributes such as Date and Time (required by FPT_STM.1), type of event, subject identifier, and outcome of the event are also part of the audit generation function.

FIA_ATD.1 provides the user and session identifiers to the audit function, so that the identity of the user who caused each event will also be recorded in the audit data (FAU_GEN.2).

The requirement FAU_SAA.1 allows administrators to determine what constitutes a potential security violation on the TOE, and allows them to apply a set of rules for monitoring audited events. When a potential security violation is detected, an annotation will be made in the audit data (FAU_ARP.1), and the administrator will be notified.

System administrators access to the audit records is covered by FAU_SAR.1$_{(CS)}$. Restricted on access to the audit records is covered by FAU_SAR.2$_{(CS)}$, whereby access to non-administrators must be explicitly granted. Formatting and sorting capabilities are covered by FAU_SAR.3 and define some of the capabilities available.

In order for the audit function to track user identities the TOE requires each user to identify itself before allowing any other TSF- mediated actions on behalf of that user, i.e. FIA_UID.2$_{(SYS)}$, and it also requires that each user be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user, FIA_UAU.2$_{(SYS)}$.

Finally, in order to protect the audit function, and to ensure its availability, FAU_STG.2 and FAU_STG.4 are required. FAU_STG.2 protects the audit data from unauthorised deletion or modification, as well as ensuring the most recent 24 hours of audit data is always maintained. In the case of an audit failure or an audit file full, no auditable events are allowed by the TOE, except those taken by an authorised administrator to remedy the situation.

This objective also supports the non-repudiation of origin requirements (FCO_NRO.2$_{(SYS)}$) by controlling access based on the identified individual. The audit logs will keep a record of all auditable events, enabling an administrator to hold individuals accountable for their actions.

O.BANNER$_{(SYS)}$ The TOE will provide a banner to notify all user that they are entering a government computer system.

The displaying of a warning message is covered by the requirement FTA_TAB.1 which states that before establishing a user session, an advisory warning message will be displayed regarding unauthorised user of the TOE.

O.CRYPTO_SUPPORT$_{(SYS)}$ The TOE must interface with cryptographic support mechanisms, that establish files and configuration parameters and ensures the integrity of these files and parameters.

These connectivity requirements are established by the CS and RU encrypting modem devices being able to exchange both user attributes (FIA_ATD.1) and specification of secrets (FIA_SOS.1). To maintain the integrity of the crypto-support mechanism, a need arises to be able to manage these security parameters (FMT_MTD.1). Also, in order to ensure the reliability of this data, trusted time stamping (FPT_STM.1) is required.

O.CS_AVAILABLE$_{(CS)}$ The CS will not allow a single user identity to connect to more than one incoming modem port at one time.

This objective is met by the requirement FRU_RSA.1$_{(CS)}$ which allows for maximum quotas on incoming CS modem ports.

O.DETECT$_{(CS)}$ The CS will detect unauthorised changes to RU configurations, when an RU connects to the CS.

The CS has the ability to detect unauthorised changes to the configuration of the RU. FAU_ARP.1 supports this by requiring the TSF to alert an administrator upon detection of a potential security violation in this system. FAU_SAA.1 further supports this objective by requiring the TSF to apply a set of rules in monitoring the auditable events and based upon these rules indicate a potential violation of the TSP.

O.IDENTIFY$_{(SYS)}$ The TOE will uniquely identify and authenticate individuals.

The TOE requires each user to identify itself before allowing any other TSF- mediated actions on behalf of that user, i.e. FIA_UID.2$_{(SYS)}$, and it also requires that each user be successfully authenticated before allowing any other TSF- mediated actions on behalf of that user, FIA_UAU.2$_{(SYS)}$.

The protection of authentication feedback, FIA_UAU.6 and FIA_UAU.7$_{(SYS)}$, and the handling of authentication failures, i.e. FIA_AFL1$_{(CS)}$ and FIA_AFL.1$_{(RU)}$, provide additional support for

O.IDENTIFY by reducing the opportunity for another individual to guess or derive from partial information a users authentication data.

This objective also supports the non-repudiation of origin requirements (FCO_NRO.2$_{(SYS)}$) by controlling access based on the identified individual. For all transmissions the individual can thus be held accountable.

O.INTEGRITY$_{(SYS)}$ The TOE will apply integrity protection to all information between the RU and the CS.

The requirement to apply both integrity and confidentiality protection to user data between the RU and CS is supported by cryptographic mechanisms as stated in FCS_COP.1. FIA_SOS.2 provides a mechanism to generate secrets that meet a minimum standard for cryptographic keys. Thus, these keys can be relied upon to provide cryptographic integrity to the data transmitted between the RU and the CS. This requirement may also be supported by the inclusion of trusted time stamping (FPT_STM) if the time stamp is used in the cryptographic hash function.

O.MANAGE$_{(SYS)}$ The TOE will provide adequate management features for its security functions.

For most of the FMT (Security Management) functions, the requirements apply to the “System” partition. There are no legitimate security management activities while the RU is in the field. When FMT requirements apply to the RU, the RU is assumed to be administered by the same administrator(s) as the CS partition.

With this interpretation and assumption, the security management functions and constraints are symmetrical across the partitions. Even though the system is physically distributed in its operational state, administrative functions only take place in a known environment. One FMT function (FMT_SAE.1, Time-limited authorisation) applies only to the CS environment. However, the effect of this function would apply to a session establishment between an RU and the CS, and so this exception does not destroy the symmetrical property of security management functions.

The FMT_SMR.1$_{(SYS)}$ component allows specific individuals to be assigned the role of administrator, so that security management functions are distinct and controllable by the TOE. This component depends upon identification of users (FIA_UID.2$_{(SYS)}$).

The FMT_MSA.1$_{(SYS)}$, FMT_MSA.2$_{(SYS)}$, and FMT_MSA.3$_{(SYS)}$ components provide controls for the management of security attributes. FMT_MSA.1$_{(SYS)}$ defines the security attributes of *user identity* and *session identifier* and restricts the ability to manage these attributes to system administrators. Users are therefore not able to affect the attributes that the P.SEPARATE and P.RECEIVE policies rely upon. The FMT_MSA.2$_{(SYS)}$ component ensures that user identities, when based on cryptographic certificates, use secure values in relation to the cryptographic algorithms implemented by the TOE. Session identifier attributes may be trivially secure. Both FMT_MSA.1$_{(SYS)}$ and FMT_MSA.2$_{(SYS)}$ depend upon system security policy definitions (FDP_IFC.1$_{(CS)}$ and FDP_IFC.1$_{(SYS)}$).

The FMT_MSA.3$_{(SYS)}$ component provides administrators to provide restrictive default values so that the default behaviour of the TOE is secure with respect to the P.SEPARATE and P.RECEIVE policies.

The FMT_MTD.1$_{(SYS)}$ component allows administrators of the system to specify TSF data that defines the use of the TOE in its operational environment. This includes generic management functions for defining valid user identities and allowable connections between RUs and the CS. These values can only be defined in the context of the TOE's operational environment. For instance, RU peripheral devices may be authorised or not, depending upon a determination of mission needs in consideration of risk exposure.

The FMT_MOF.1$_{(SYS)}$ component further defines the controls on security functions of the TOE that are to be available for administrators. The administrative controls specified in this component are appropriate for managing systems providing strong I&A and basic communications functionality, and which process SBU data.

The FMT_SAE.1$_{(CS)}$ component allows administrators to specify expiration times for user identities within the system. This function limits the exposure of attacks based on circumventing controls on user identities. For instance, when user identity is based on cryptographic certificates, the certificate might have a limited valid lifetime or might somehow become invalid over time. This component depends upon reliable time stamps (FPT_STM.1$_{(CS)}$).

Similarly, the FMT_REV.1$_{(SYS)}$ component provides for immediate, on-demand invalidation of a user's identity. This function is used for either normal termination of a user's authorisation to the TOE or when a particular user's behaviour becomes suspicious to administrators. Revocation could occur while the user already has a session established. It is not clear that immediate suspension of user activity is always desirable when an identity is revoked (e.g., for normal termination of an account). However, it is reasonable to assume that trivial, manual procedures—including drastic measures such as rebooting the CS—are available to administrators that want to immediately end a user's activity with the TOE.

O.MEDIA$_{(RU)}$ The RU will protect data stored on the unit while it is not in use and unattended.

FCS_COP.1$_{(RU)}$ provides a function to encrypt all user data on the RU disk. FDP_RIP.2$_{(RU)}$ provides eradication of data on the RU when administrators issue the RU to a different user who may not have access to the information of the previous user. If an authorized user is connected in a remote session to the CS, and steps away from the terminal for a period of time, the session locking requirement (FTA_SSL.1$_{(RU)}$) will prevent an unauthorized user from using the terminal.

O.NO_EAVESDROP$_{(SYS)}$ The TOE will prevent, with a strength appropriate for tunnelling SBU data across a public network, the disclosure of information during transfers between an RU and the CS.

All data transmitted over the TN is encrypted using a cryptographic system appropriate for SBU (Type II) information (FCS_COP.1$_{(CS)}$ and FCS_COP.1$_{(RU)}$), including key generation, distribution, and destruction (FCS_CKM.1$_{(SYS)}$, FCS_CKM.2$_{(SYS)}$, and FCS_CKM.4$_{(SYS)}$). The TOE will also prevent the disclosure or modifications of user data when transmitted between the RU and CS (FDP.ITT.1(SYS)).

O.RECEIVE$_{(SYS)}$ A CS or a RU will only accept remote commands and data from another CS or RU with which it is mutually authenticated.

By the P.RECEIVE policy, remote commands and data are only accepted by a CU or a RU from another CU or RU if the RU is registered with the CU (FDP_IFC.1$_{(SYS)}$ and FDP_IFF.1$_{(SYS)}$). Mutual cryptographic authentication between a CU and a RU (FCS_COP.1$_{(CS)}$ and FCS_COP.1$_{(RU)}$) must occur before any data can be exchanged between the CS and RU.

This objective also provides partial support for the non-repudiation of origin requirement (FCO_NRO.2$_{(SYS)}$) by limiting transmissions to authorized RUs and CSs.

O.SECURE_STARTUP$_{(SYS)}$ Upon initial start-up of the TOE or recovery from an interruption in TOE services, the TOE must default to a secure state and not compromise its files, configuration parameters, or information being processed before the interruption occurred.

Upon detection of a failure or recovery from an interruption the TOE will first attempt to automatically recover (FPT_RCV.2). Should recovery not be possible it will return to a secure state.

O.SELF-PROTECT$_{(SYS)}$ The TOE will protect its security-related functions against external interference or tampering by users, or attempts by users to bypass its security functions.

Within the RU and the CS, the TSF shall ensure that TSP enforcement functions are invoked and succeed before each function within the TSC is allowed to proceed (FPT_RVM.1$_{(SYS)}$). It shall maintain a security domain for its own execution that protects it from interference and tampering by untrusted subjects (FPT_SEP.1$_{(SYS)}$). While TSF data is in transit over the TN, it shall be protected from modification, disclosure, or replay (FPT_ITT.2$_{(SYS)}$, FPT_ITT.3$_{(SYS)}$, and FPT_RPL.1$_{(SYS)}$).

O.SELF_TEST$_{(SYS)}$ The TOE will perform self-tests of its security functions including those required by the site security policy and site procedures.

Requirements to perform designated self testing during initial start-up, periodically and at the request of an authorized administrator result from the inclusion of the Underlying Abstract Machine Test requirement (FPT_AMT). The ability to test the integrity of both TSF and TSF executable code is driven by the requirement TSF Self Test (FPT_TST). The inclusion of the requirement Specification of Secrets (FIA_SOS) drives a self-testing need for the TOE to verify the appropriateness of key length, randomness, etc.

OE.BACKUP$_{(CS)}$ The requirement FAU_STG.4 protects the backup of all audit data against unauthorised deletion. FAU_STG.2 protects the stored audit records from unauthorised deletion or modification, and guarantees the most recent 24 hours of audit records will be maintained. Other TSF data (e.g., ACL, configuration files) are protected against modification or deletion by the requirement FMT_MTD.1

OE.INSTALL$_{(SYS)}$ The remote access system will be delivered, installed, and managed in a manner which maintains the system security.

The remote access system will be delivered, installed, and managed in a manner which maintains the system security. This objective is met primarily through requirements on the environment and administrator. The environmental requirement ITR.INSTALL$_{(SYS)}$ satisfies this objective. FMT_MOF.1 and FMT_MSA.3 provide for management functions to maintain system security. EAL 2 specifies the appropriate assurance requirements to ensure the TSF has met the necessary developmental, operational and maintenance aspects of the TOE.

OE.PHYSICAL$_{(SYS)}$ TOE hardware, software, and documentation, and all classified data handled by the TOE will be physically protected to prevent unauthorised (intentional or unintentional) disclosure.

It is assumed that all TOE components will be physically protected to the degree commensurate with the level of the information processed by in the TOE as provided by the environmental requirement NITR.PHYSICAL$_{(CS)}$.

OE.REVIEW$_{(CS)}$ Administrators will periodically review audit trail information.

FAU_SAR.1, FAU_SAR.2 and FAU_SAR.3 enable audit review by the administrator including the ability to perform searches, sorting and ordering of audit data. The administrator is expected to review the TOE audit records periodically to maintain a secure environment. Lack of review of the audit features, could inadvertently open a vulnerability in the TOE. ITR.REVIEW$_{(CS)}$ supports this objective in that there is a requirement for the administrator to be responsive to security alarms and review audit records.

OE.TRAIN$_{(SYS)}$ Authorised users and administrators are trained as to establishment and maintenance of sound security policies and practices.

All users and administrators of the remote access system are expected to be trained in proper operation of the system. Failure to conduct proper training on the operation of the security attributes and functions of the system could result in failure of the TSF. The non-IT requirement NITR.TRAINING identifies the need for an effective training plan to be established to support the proper use and operation of the remote access system.

6.3.2 Assurance Security Requirements Rationale

The assurance requirements for the SBU Remote Access System are found in EAL 2, augmented with ADV_SPM.1 Informal TOE security policy model. The Global Information Grid (GIG) Policy (DoD Policy Memorandum No. 6-8510) states that mission support systems should meet a basic level of robustness for all identified security services. The GIG Policy Implementation Guidance states that Basic robustness means a minimum of EAL 1. For the SBU Remote Access system, the assurance level has been increased slightly to reflect the importance of protecting DoD SBU information. An SBU remote access system may potentially have to protect the most sensitive SBU information, therefore this PP calls for an EAL 2.

6.4 Dependency Rationale

Table 6-3. Functional and Assurance Requirements Dependencies

Requirement	Dependencies	
Functional Requirements		
FAU_ARP.1$_{(SYS)}$	FAU_SAA.1	
FAU_GEN.1	FPT_STM.1	
FAU_GEN.2	FAU_GEN.1	FAU_UID.1
FAU_SAA.1	FAU_GEN.1	

Requirement	Dependencies
FAU_SAA.3$_{(CS)}$	None
FAU_SAR.1	FAU_GEN.1
FAU_SAR.2	FAU_SAR.1
FAU_SAR.3	FAU_SAR.1
FAU_STG.1	FAU_GEN.1
FAU_STG.2	FAU_GEN.1
FAU_STG.4	FAU_STG.1
FCO_NRO.2	FIA_UID.1
FCS_CKM.1	FCS_CKM.2 FCS_COP.1 FCS_CKM.4 FMT_MSA.2
FCS_CKM.2	FDP_ITC.1 FCS_CKM.1 FCS_CKM.4 FMT_MSA.2
FCS_CKM.4	FDP_ITC.1 FCS_CKM.1 FMT_MSA.2
FCS_COP.1$_{(RU)}$ FCS_COP.1$_{(CS)}$	FDP_ITC.1 FCS_CKM.1 FCS_CKM.4 FMT_MSA.2
FDP_ACC.1$_{(RU)}$	FDP_ACF.1
FDP_ACF.1	FDP_ACC.1 FMT_MSA.3
FDP_IFC.1$_{(SYS)}$ FDP_IFC.1$_{(CS)}$	FDP_IFF.1
FDP_IFF.1$_{(CS)}$ FDP_IFF.1$_{(SYS)}$	FDP_IFC.1 FMT_MSA.3
FDP_ITT.1	FDP_ACC.1 FDP_IFC.1
FDP_ITT.3$_{(SYS)}$	FDP_ACC.1 FDP_IFC.1 FDP_ITT.1
FDP_RIP.2$_{(RU)}$	None
FDP_SDI.2	None
FIA_AFL.1$_{(CS)}$ FIA_AFL.1$_{(RU)}$	FIA_UAU.1
FIA_SOS.1	None
FIA_SOS.2	None
FIA_UAU.2$_{(SYS)}$	FIA_UID.1
FIA_UAU.6	None
FIA_UAU.7$_{(SYS)}$	FIA_UAU.1
FIA_UID.2$_{(SYS)}$	None
FIA_USB.1$_{(CS)}$	FIA_ATD.1
FMT_MOF.1$_{(SYS)}$	FMT_SMR.1

Requirement	Dependencies
FMT_MOF.1$_{\text{(RU)}}$	
FMT_MSA.1$_{\text{(SYS)}}$	FDP_ACC.1 FDP_IFC.1 FMT_SMR.1
FMT_MSA.2$_{\text{(SYS)}}$	ADV_SPM.1 FDP_ACC.1 FDP_IFC.1 FMT_MSA.1 FMT_SMR.1
FMT_MSA.3$_{\text{(SYS)}}$	None
FMT_MTD.1$_{\text{(SYS)}}$	FMT_SMR.1
FMT_REV.1$_{\text{(SYS)}}$	FMT_SMR.1
FMT_SAE.1$_{\text{(CS)}}$	FMT_SMR.1 FPT_STM.1
FMT_SMR.1$_{\text{(SYS)}}$	FIA_UID.1
FPT_AMT.1	None
FPT_ITT.2$_{\text{(SYS)}}$	None
FPT_ITT.3$_{\text{(SYS)}}$	FPT_ITT.1
FPT_RPL.1$_{\text{(SYS)}}$	None
FPT_RVM.1$_{\text{(SYS)}}$	None
FPT_SEP.1$_{\text{(SYS)}}$	None
FPT_STM.1$_{\text{(CS)}}$	None
FPT_TST.1	FPT_AMT.1
FRU_RSA.1	None
FTA_SSL.1	FIA_UAU.1
FTA_TAB.1$_{\text{(SYS)}}$	None
ITR_INSTALL	None
ITR_REVIEW	None
NITR_PHYSICAL	None
NITR_TRAINING	None
Assurance Requirements	
ACM_CAP.2	None
ADO_DEL.1	None
ADO_IGS.1	AGD_ADM.1
ADV_FSP.1	ADV_RCR.1
ADV_HLD.1	ADV_FSP.1 ADV_RCR.1
ADV_RCR.1	None
AGD_ADM.1	ADV_FSP.1
AGD_USR.1	ADV_FSP.1
ATE_COV.1	ADV_FSP.1 ATE_FUN.1

Requirement	Dependencies
ATE_FUN.1	None
ATE_IND.2	ADV_FSP.1 AGD_ADM.1 AGD_USR.1
AVA_SOF.1	ADV_FSP.1 ADV_HLD.1
AVA_VLA.1	ADV_FSP.1 ADV_HLD.1 AGD_ADM.1 AGD_USR.1

6.5 Security Functional Requirements Grounding in Objectives

Table 6-4. Requirements to Objectives Mapping

Requirements	Objectives
FAU_ARP.1	O.DETECT$_{(CS)}$ O.AUDIT$_{(CS)}$
FAU_GEN.1	O.AUDIT$_{(CS)}$
FAU_GEN.2	O.AUDIT$_{(CS)}$
FAU_SAA.1	O.AUDIT$_{(CS)}$
FAU_SAA.3	O.DETECT$_{(CS)}$
FAU_SAR.1	O.AUDIT$_{(CS)}$ O.MANAGE$_{(SYS)}$ OE.REVIEW$_{(CS)}$
FAU_SAR.2	O.AUDIT$_{(CS)}$ O.MANAGE$_{(SYS)}$ OE.REVIEW$_{(CS)}$
FAU_SAR.3	O.AUDIT$_{(CS)}$ O.MANAGE$_{(SYS)}$ OE.REVIEW$_{(CS)}$
FAU_STG.1	O.AUDIT$_{(CS)}$
FAU_STG.2	OE.BACKUP$_{(CS)}$
FAU_STG.4	O.AUDIT$_{(CS)}$ OE.BACKUP$_{(CS)}$
FCO_NRO.2	O.AUDIT$_{(CS)}$ O.IDENTIFY$_{(SYS)}$ O.RECEIVE$_{(SYS)}$ O.ACCESS$_{(SYS)}$
FCS_CKM.1	O.NO_EAVESDROP$_{(SYS)}$
FCS_CKM.2	O.NO_EAVESDROP$_{(SYS)}$
FCS_CKM.4	O.NO_EAVESDROP$_{(SYS)}$
FCS_COP.1	O.MEDIA$_{(RU)}$ O.NO_EAVESDROP$_{(SYS)}$ O.RECEIVE$_{(SYS)}$ O.INTEGRITY$_{(SYS)}$
FDP_ACC.1	O.ACCESS$_{(RU)}$
FDP_ACF.1	O.ACCESS$_{(RU)}$
FDP_IFC.1	O.ACCESS$_{(SYS)}$ O.RECEIVE$_{(SYS)}$
FDP_IFF.1	O.ACCESS$_{(SYS)}$ O.RECEIVE$_{(SYS)}$
FDP_ITT.1	O.NO_EAVESDROP$_{(SYS)}$

Requirements	Objectives		
FDP_ITT.3	O.ACCESS$_{(SYS)}$		
FDP_RIP.2	O.MEDIA$_{(RU)}$	O.ACCESS$_{(RU)}$	
FDP_SDI.2	O.ANTIVIRUS$_{(SYS)}$		
FIA_AFL.1	O.IDENTIFY$_{(SYS)}$		
FIA_ATD.1	O.CRYPTO_SUPPORT$_{(SYS)}$		
FIA_SOS.1	O.SELF_TEST$_{(SYS)}$	O.CRYPTO_SUPPORT$_{(SYS)}$	
FIA_SOS.2	O.SELF_TEST$_{(SYS)}$	O.INTEGRITY$_{(SYS)}$	
FIA_UAU.2	O.ACCESS$_{(RU)}$	O.AUDIT$_{(CS)}$	O.IDENTIFY$_{(SYS)}$
FIA_UAU.6	O.ACCESS$_{(RU)}$	O.IDENTIFY$_{(SYS)}$	
FIA_UAU.7	O.IDENTIFY$_{(SYS)}$		
FIA_UID.2	O.IDENTIFY$_{(SYS)}$		
FIA_USB.1	O.AUDIT$_{(CS)}$		
FMT_MOF.1	O.MANAGE$_{(SYS)}$	OE.INSTALL$_{(SYS)}$	
FMT_MSA.1	O.MANAGE$_{(SYS)}$		
FMT_MSA.2	O.MANAGE$_{(SYS)}$		
FMT_MSA.3	O.MANAGE$_{(SYS)}$	OE.INSTALL$_{(SYS)}$	
FMT_MTD.1	O.MANAGE$_{(SYS)}$	OE.BACKUP$_{(CS)}$	O.CRYPTO_SUPPORT$_{(SYS)}$
FMT_REV.1	O.MANAGE$_{(SYS)}$		
FMT_SAE.1	O.MANAGE$_{(SYS)}$		
FMT_SMR.1	O.MANAGE$_{(SYS)}$		
FPT_AMT.1	O.SELF_TEST$_{(SYS)}$		
FPT_ITT.2	O.SELF_PROTECT$_{(SYS)}$		
FPT_ITT.3	O.SELF_PROTECT$_{(SYS)}$		
FPT_RCV.2	O.SECURE_STARTUP$_{(SYS)}$		
FPT_RPL.1	O.SELF_PROTECT$_{(SYS)}$		
FPT_RVM.1	O.SELF_PROTECT$_{(SYS)}$		
FPT_SEP.1	O.SELF_PROTECT$_{(SYS)}$		
FPT_STM.1	O.AUDIT$_{(CS)}$	O.CRYPTO_SUPPORT$_{(SYS)}$	
FPT_TST.1	O.SELF_TEST$_{(SYS)}$		
FRU_RSA.1	O.CS_AVAILABLE$_{(CS)}$		
FTA_SSL.1	O.ACCESS$_{(RU)}$	O.ACCESS$_{(SYS)}$	O.MEDIA$_{(RU)}$
FTA_TAB.1	O.BANNER$_{(SYS)}$		
ITR_INSTALL	OE.INSTALL$_{(SYS)}$		

Requirements	Objectives
ITR_REVIEW	OE.REVIEW$_{(CS)}$
NITR_PHYSICAL	OE.PHYSICAL$_{(SYS)}$
NITR_TRAINING	OE.TRAIN$_{(SYS)}$

6.6 Explicit Requirements Rationale

As shown in Table 6-4 ITR_INSTALL, ITR_REVIEW, NITR_PHYSCIAL, and NITR_TRAINING were added because the common criteria doesn't cover environmental requirements. Environmental objectives must be met when dealing with a remote access system.

Appendix A — Acronyms

CC	Common Criteria
CS	Communications Server
EAL	Evaluation Assurance Level
IATF	Information Assurance Technology Framework
ISSE	Information System Security Engineers
IT	Information Technology
LAN	Local Area Network
PP	Protection Profile
PSTN	Public Switched Telephone Network
RU	Remote Unit
SBU	Sensitive But Unclassified
SF	Security Function
SFP	Security Function Policy
SOF	Strength of Function
ST	Security Target
SYS	System
TN	Telephone Network
TOE	Target of Evaluation
TSC	TSF Scope of Control
TSF	TOE Security Functions
TSFI	TSF Interface
TSP	TOE Security Policy

References

Common Criteria Implementation Board, *Common Criteria for Information technology Security Evaluation*, CCIB-98-026, Version 2.0, May 1998